ISO27k Toolkit

ISMS Auditing Guideline

Version 2, 2017

Generic, pragmatic guidance for auditing an organization's ISO27k **I**nformation **S**ecurity **M**anagement **S**ystem, covering both the *management system* and the *information security controls*.

A template for internal audit use by IT auditors, written by and for practitioners.

Complements the ISO27k (ISO/IEC 27000-series) international standards on information security.

Information Security Management System Auditing Guideline

Prepared by practitioners from the ISO27k Forum

Version 2 August 2017

Contents

1. Introduction 5

2. Scope and purpose of this guideline 5

3. References 5

4. Terms and definitions 6

5. Principles of auditing 7

6. Audit management 8

6.1 Managing the ISMS audit programme 8

6.2 Managing an ISMS audit 8

7. The audit process 9

7.1 Scoping and pre-audit survey 9

7.2 Audit planning and preparation 10

7.3 Audit fieldwork 10

7.4 Audit analysis 11

7.5 Audit reporting 11

7.6 Audit closure 13

8. Competence and evaluation of auditors 13

8.1 Auditor competence 13

8.2 Demonstration of auditor competence 14

9. Document control 15

9.1 Authors 15

9.2 History 15

9.3 Feedback 15

9.4 Copyright 15

Appendix A - Generic *information security* audit checklist **16**
Introduction 16
A.5. Information security policies 17
A.6. Organisation of information security 17
A.6.1 Internal organisation 17
A.6.2 Mobile devices and teleworking 19
A.7. Human resources security 19
A.7.1 Prior to employment 19
A.7.2 During employment 19
A.7.3 Termination and change of employment 20
A.8. Asset management 20
A.8.1 Responsibility for assets 20
A.8.2 Information classification 22
A.8.3 Media handling 22
A.9 Access control 23
A.9.1 Business requirements of access control 23
A.9.2 User access management 23
A.9.3 User responsibilities 24
A.9.4 System and application access control 25
A.10. Cryptography 25
10.1 Cryptographic controls 25
A.11. Physical and environmental security 26
A.11.1 Secure areas 26
A.11.2 Equipment 27
A.12. Operations security 29
A.12.1 Operational procedures and responsibilities 29
A.12.2 Protection from malware 30
A.12.3 Backup 31
A.12.4 Logging and monitoring 31
A.12.5 Control of operational software 32
A.12.6 Technical vulnerability management 32
A.12.7 Information systems audit considerations 32
A.13. Communications security 33
A.13.1 Network security management 33
A.13.2 Information transfer 33
A.14. System acquisition, development and maintenance 34

A.14.1 Security requirements of information systems 34

A.14.2 Security in development and support processes 34

A.14.3 Test data 36

A.15. Supplier relationships 36

A.15.1 Information security in supplier relationships 36

A.15.2 Supplier service delivery management 37

A.16. Information security incident management 37

A.16.1 Management of information security incidents and improvements 37

A.17. Business continuity management (per ISO 22301) 39

A.17.1 Business continuity 39

A.17.2 Redundancies 39

A.18. Compliance 40

A.18.1 Compliance with legal and contractual requirements 40

A.18.2 Information security reviews 41

Appendix B - Generic ISMS *management system* audit checklist 42

Introduction 42

B.4. Context of the organization 43

B.4.1 Understanding the organization and its context 43

B.4.2 Understanding the needs and expectations of interested parties 43

B.4.4 Information Security Management System 43

B.5. Leadership 44

B.5.1 Leadership and commitment 44

B.5.2 Policy 44

B.5.3 Organizational roles, responsibilities and authorities 45

B.6. Planning 45

B.6.1 Actions to address risks and opportunities 45

B.6.2 Information security objectives and planning to achieve them 46

B.7. Support 46

B.7.1 Resources 46

B.7.2 Competence 46

B.7.3 Awareness 47

B.7.4 Communication 47

B.7.5 Documented information 47

B.8. Operation 48

B.8.1 Operational planning and control 48

B.8.2 Information security risk assessment 48
B.8.3 Information security risk treatment 48
B.9. Performance evaluation 49
B.9.1 Monitoring, measurement, analysis and evaluation 49
B.9.2 Internal audit 50
B.9.3 Management review 50
B.10. Improvement 50
B.10.1 Nonconformity and corrective action 50
B.10.2 Continual improvement 51

1. Introduction

This **I**nformation **S**ecurity **M**anagement **S**ystem auditing guideline is maintained by members of the ISO27k Forum at ISO27001security.com, an international community of practitioners who are actively using the ISO/IEC 27000-family of ISMS standards known colloquially as "**ISO27k**".

We wrote this initially in 2008 to contribute to the development of ISO/IEC 27007 by providing what we, as experienced ISMS implementers and IT/ISMS auditors, believed to be worthwhile content. A secondary aim was to provide a pragmatic and useful guideline for those involved in auditing ISMSs.

Since then, ISO/IEC 27007 has been published. Other ISO27k standards have been revised as well, so the guideline was thoroughly updated in 2017.

The main body of this guideline concerns the purpose and process of auditing. Appendix A is a checklist (a generic set of audit tests) for auditing the *information security controls* being managed by the ISMS. Appendix B is a checklist for auditing the *management system* itself.

2. Scope and purpose of this guideline

This guideline provides general advice to IT auditors reviewing ISMSs against the ISO27k standards, principally ISO/IEC 27001:2013 (the certification standard specifying the **management system**) and ISO/IEC 27002:2013 (the code of practice recommending a suite of **information security controls**).

This guideline is particularly aimed at those performing ISMS internal audits and management reviews – **not** formal certification audits. The guidance needs to be interpreted or tailored to specific situations. Audits are normally risk-based, providing a natural priority to the ISMS audit work reflecting business requirements for information risk and security management.

Explanatory notes, tips and warnings are scattered throughout the guideline in text boxes.

3. References

Please refer to:

- **ISO/IEC 27000:2016** *Information technology — Security techniques — Information security management systems - Overview and vocabulary.* This free standard provides an overview of ISO27k and formally defines many specialist terms used in the standards.
- **ISO/IEC 27001:2013** *Information technology — Security techniques — Information security management system requirements*. This is the formal specification for an ISMS against which organizations may be certified compliant. Section 6 introduces the need for 'Internal ISMS audits' and briefly sets the main requirements for audit procedures. Section 7 also identifies the need for periodic (at least annual) management reviews of the ISMS. Other than the controls listed in Annex A, these are mandatory requirements for certified organizations. Even if the organization implements an alternative control set, the chosen controls must be checked against those listed in Annex A for relevance and completeness.
- **ISO/IEC 27002:2013** *Information technology — Security techniques — Code of practice for information security controls*. Expands substantially on ISO/IEC 27001 Annex A.
- **ISO/IEC 27003:2017** *Information technology — Security techniques — Information security management system — Guidance.* Further, practical guidance on designing and implementing a workable ISMS.

- **ISO/IEC 27004:2016** *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation.* Guidance on selecting/developing and using metrics to manage information risk and security rationally and proportionately.
- **ISO/IEC 27006:2015** *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*. Formal accreditation criteria for certification bodies conducting strict compliance audits against ISO/IEC 27001.
- **ISO/IEC 27007:2011** *Information technology — Security techniques — Guidelines for information security management systems auditing.* Guidance for accredited certification bodies, internal auditors, external/third party auditors and others conducting compliance auditing of the *management system* parts of ISMSs against ISO/IEC 27001.
- **ISO/IEC TR 27008:2011** *Information technology — Security techniques — Guidelines for auditors on information security controls.* Guidance for internal auditors and others auditing or reviewing the *information security* aspects of ISMSs.
- **ISO/IEC 27017:2015** *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.* Covers information security controls for cloud computing.
- Other ISO27k and related standards. This growing suite of ISMS-related standards provides a wealth of sound advice on information risk and security, cybersecurity, cloud security, business continuity (*e.g*. ISO 22301) and other topics.
- **ISO/IEC 17021-1:2015** *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements.* Guidance on compliance audits by certification bodies ("third party" audits).
- **ISO 19011:2011** *Guidelines for auditing management systems.* Guidance on internal audits ("first party") and supplier audits ("second party").
- The IT Audit FAQ has general advice on conducting IT audits, auditor qualifications and competencies, audit process *etc.*
- ISACA offers professional guidance and support to IT audit professionals.
- The Institute of Internal Auditors supports internal auditors of all kinds.

4. Terms and definitions

Most ISMS-related terms used in this guide and in related standards are defined in ISO/IEC 27000 and ISO 19011. Specific IT and ISMS audit-related terms are defined here for clarity, as they are interpreted and used in this guideline:

- **Audit** - the process by which an audit subject is independently reviewed and reported on by one or more competent auditors on behalf of stakeholders. Audit is a systematic, independent, formal, structured and documented process for obtaining audit evidence and testing it objectively to determine the extent to which the audit criteria are fulfilled;
- **Audit checklist** - a structured questionnaire or workplan to guide the auditors in testing the audit subject;
- **Audit criteria** - used as a reference for the audit. May include requirements or goals that the ISMS should fulfil (*e.g.* compliance with relevant ISO27k standards, corporate policies and procedures, laws and regulations, contractual obligations *etc.*), and issues or anti-goals that the ISMS should avoid (*e.g.* inefficiencies such as excessive business costs and inappropriate, unnecessary or ineffective activities);

- **Audit evidence** - verifiable, fact-based information gathered from the area being audited such as written documentation (*e.g.* policies, computer printouts, completed forms, reports), interview notes or recordings, and other observations (*e.g*. photographs of physical security issues);
- **Audit finding** - the auditor's summary/description and analysis of an inadequately mitigated information risk;
- **Audit observation** (also called **O**pportunity **f**or **I**mprovement) - advice which carries less weight than an audit recommendation, such as a suggestion which - if ignored - may lead to a nonconformity or some other business impact (*e.g.* sub-optimal processes or systems);
- **Audit plan or programme** - a project plan for an audit laying out the main audit activities and their timing;
- **Audit recommendation** - a corrective action that is proposed to address one or more identified audit findings, that must be addressed prior to certification or recertification of the ISMS;
- **Audit report** - a formal report to management documenting the key findings and conclusions of the audit. Usually a written document but may also involve a presentation and discussion;
- **Audit risk** - the potential for an audit to fail to meet its objectives, for example by using unreliable, incomplete or inaccurate information, or failing to address significant issues in sufficient depth;
- **Audit schedule** - a diary of planned audits;
- **Audit scope or subject** - the organization/s, or parts of an organization, which are being audited;
- **Audit test** - a check conducted by the auditor to verify whether a control is effective, efficient and adequate to mitigate one or more information risks;
- **Audit work papers** - information written and gathered by the auditor recording their examination, findings and analysis of the ISMS, such as completed audit checklists;
- **Compliance audit** - a type of audit specifically designed to assess the extent to which the audit subject satisfies stated requirements;
- **ISMS audit** - an audit centred on an **I**nformation **S**ecurity **M**anagement **S**ystem;
- **Risk-based audit** - an audit planned and conducted on the basis of an assessment of risks - specifically information risks in the ISO27k context, plus audit and other risks such as health and safety;
- **Workers** – a deliberately vague term includes full and part-time employees of the organization (staff and managers) *plus* contractors, consultants, advisors, maintenance and support technicians, temps, interns/students and others working directly within, for and/or under the control of the organization.

5. Principles of auditing

ISO 19011 section 4 covers the principles of auditing in general, including important generic audit principles *e.g.* independent evaluation against agreed criteria, plus more specific principles aimed at management systems audits. In all matters related to the audit, the auditor should be independent in both attitude and appearance. The audit function or team should be independent of the area or activity being reviewed to permit objective completion of the audit assignment.

Independence is as much about the auditor's state of mind as reporting relationships: objective, rational, critical thinking enables the auditor to notice things that others miss or ignore.

6. Audit management

6.1 Managing the ISMS audit programme

Managing a programme of ISMS audits involves planning, controlling and monitoring/overseeing it, through activities such as:

- Prioritizing, planning and outlining the scope of individual ISMS audits within the overall audit work programme, perhaps combining wide-scope superficial ISMS audits with more tightly-focused audits going to more depth on areas of particular concern (*e.g*. longstanding issues or significant risks);
- Allocating suitable resources to undertake planned and approved audits (*e.g.* ensuring that ISMS auditors are trained, competent and motivated to do the work to a required level of quality);
- Arranging or coordinating ISMS audits at multi-site organizations including multinationals and 'group' structures, where comparisons between the ISMSs in operation within individual business units can help share and promote good practices;
- Auditing the ISMSs of second parties such as suppliers and business partners (note: a second party's ISO/IEC 27001 certification from an accredited certification body may or may not provide sufficient assurance across all the areas of concern, for example there may be significant information risks or compliance implications arising from information services provided, or incidents and concerns may indicate issues that deserve exploring).

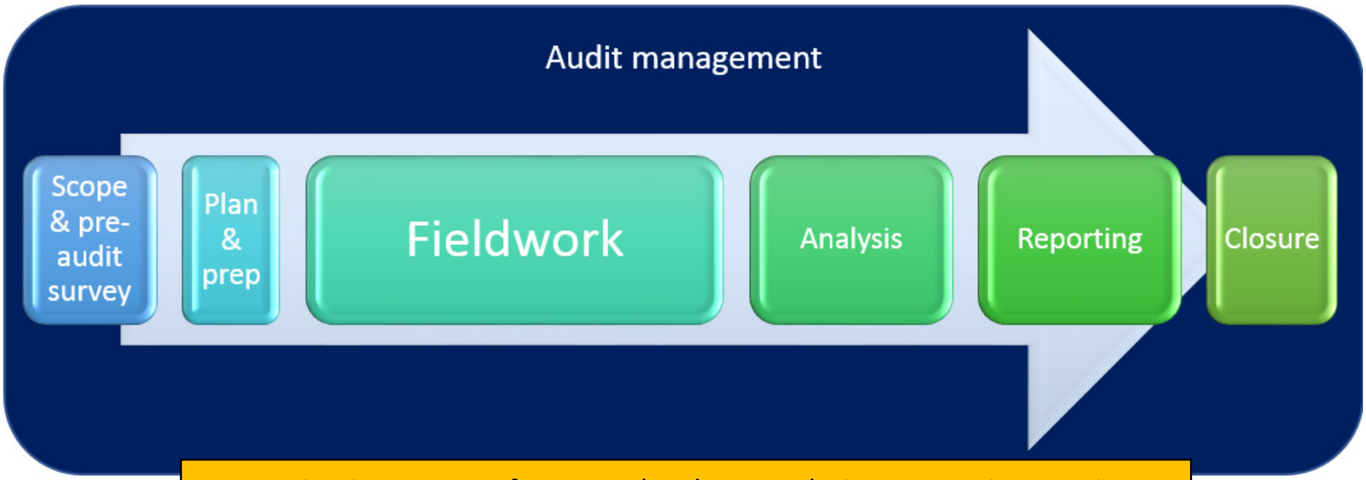
6.2 Managing an ISMS audit

Each ISMS audit is managed throughout the process shown in section 7. Audit management activities include:

- Gaining support from management to conduct the ISMS audit as proposed in outline, with their agreement in principle and authority to proceed with the detailed scoping and planning (which may lead to a further authorization step once finalized);
- Supervising, guiding, motivating and supporting auditors, ensuring they follow accepted audit practices, conducting file reviews and proofreading draft reports;
- Reviewing and challenging unsubstantiated or notable findings *e.g.* playing the devil's advocate to explore the evidence, depth of analysis and nature of issues; proposing alternative explanations and potential recommendations; helping auditors evaluate the risks in the business context;
- Dealing with issues that jeopardize the audit assignment such as interpersonal problems, lack of engagement, delays, reluctance or refusal to supply essential information *etc*. (issues may be raised or escalated by anyone involved in the process);
- Liaising with management, perhaps providing interim updates and setting expectations for the audit reporting phase.

7. The audit process

While the phase names and details vary, audit assignments typically follow a logical sequence along these lines:



Iteration is common, for example where analysis or reporting requires additional evidence, more fieldwork may be performed.

7.1 Scoping and pre-audit survey

During this phase, ISMS auditors determine the main area/s of focus for the audit and any areas that are explicitly out-of-scope, based normally on an initial risk-based assessment plus discussion with those who commissioned the ISMS audit.

Information sources include: general research on the industry and the organization, plus the ISO27k standards and good security practices, previous ISMS audit and management review reports (and others where relevant), and ISMS documents such as the **S**tatement **o**f **A**pplicability, **R**isk **T**reatment **P**lan and ISMS policies.

ISMS auditors should ensure that the audit scope 'makes sense' in relation to the organization. It should normally match the scope of the ISMS. For example, large organizations with multiple divisions or business units may have separate ISMS's, an all-encompassing enterprise-wide ISMS, or some combination of local and centralized ISMS. If the ISMS covers the entire organization, the auditors may need to review the ISMS in operation at all - or at least a representative sample of - business locations, such as the headquarters and a selection of discrete business units, departments, sites *etc*. of their choosing.

The auditors should pay particular attention to information risks and security controls associated with information conduits to other entities (organizations, business units *etc*.) that fall outside the scope of the ISMS, for example checking the adequacy of information security-related clauses in Service Level Agreements or contracts with IT service suppliers.

This should be easier where the out-of-scope entities have themselves been certified compliant with ISO/IEC 27001.

During the pre-audit survey, the ISMS auditors identify and ideally make contact with the main stakeholders in the ISMS such as the CISO, information risk and security manager/s and influential figures such as the CIO and CEO, plus other professionals such as security architects and security administrators; IT, HR, facilities and physical security professionals; ISMS developers and implementers … perhaps taking the opportunity to request pertinent documentation *etc*. that will be reviewed during the audit.

Management normally nominates one or more audit “escorts” - individuals who are responsible for ensuring that the auditors can move freely about the organization and rapidly find the people, information *etc*. necessary to conduct their work, acting as guides, facilitators and management liaison points.

The primary output of this phase is an **ISMS audit scope, charter, engagement letter or similar**, agreed between the auditors and client management. Contact lists and other preliminary documents are also obtained and the audit files are opened to contain documentation (audit working papers, evidence, notes, feedback, draft and final reports *etc*.) arising from the audit.

7.2 Audit planning and preparation

The agreed ISMS scope is broken down into greater detail, typically by generating an ISMS audit checklist (please see the appendices for two detailed but generic examples).

The overall timing and resourcing of the audit is negotiated and agreed by management of both the organization being audited and the ISMS auditors, in the form of an audit plan or schedule. Conventional project planning techniques (such as GANTT charts showing phases, durations, milestones *etc*.) are helpful.

Audit plans identify and put broad boundaries around the remaining phases of the audit (*e.g*. timescales). It is common at this stage to make preliminary bookings for the formal audit report/discussion meeting due at the end of the audit to allow senior participants to schedule their attendance.

Audit plans often also include “checkpoints” - specific opportunities for the auditors to provide informal interim updates to their management contacts including preliminary notification of any observed inconsistencies or potential nonconformities *etc*. These are also opportunities to raise any concerns over limited access to information or people, and for management to raise any concerns over the nature of the audit work. While auditors are necessarily independent, they must establish a level of trust and a cooperative working environment in order to engage sufficiently and obtain the information necessary to audit the ISMS. Professional approach, competence and integrity are crucial.

The checklists in this guideline are **not** intended to be used without due consideration and modification. This is merely guidance. Auditors normally generate custom checklists reflecting the specific scope and scale of the particular ISMS being audited, taking into account relevant requirements that are already evident at this stage (such as information security related laws, regulations and standards that are commonly known in the industry).

Finally, the timing of important audit work elements may be determined, particularly in order to prioritize aspects that are believed to represent the greatest risks to the organization if the ISMS are found to be inadequate.

The output of this phase is the (customized) audit checklist and an audit plan agreed with management.

7.3 Audit fieldwork

This is generally the longest phase of an audit although reporting can also be lengthy.

During audit fieldwork, audit evidence is gathered by the auditor/s working methodically through the audit checklist, for example interviewing staff, managers and other stakeholders associated with the ISMS, reviewing ISMS documents, printouts and data (including records of ISMS activities such as security log reviews), observing ISMS processes in action and checking system security configurations *etc*. Audit tests are performed to evaluate and validate the evidence as it is gathered. Audit work papers are prepared, documenting the tests performed, evidence gathered and initial results.

The first part of the fieldwork typically involves a documentation review. The auditor reads and makes notes about documentation relating to and arising from the ISMS (such as the Statement of Applicability, Risk Treatment Plan, ISMS policy *etc.*). The auditor generates audit documentation comprising of audit evidence and notes in the form of completed audit checklists and working papers.

Audit checklists may be modified further *during* the course of audits *e.g.* if previously underappreciated areas of concern come to light, or if it is appropriate to change the emphasis or level of detail as a result of information obtained. Even the audit scope may be modified, provided the change is justified to and approved by management.

Findings from the documentation review often indicate the need for specific audit tests to determine how closely the ISMS as currently implemented follows the documentation, as well as testing the general level of compliance and testing appropriateness of the documentation in relation to ISO/IEC 27001. Typical audit tests are shown in Appendix A and Appendix B. The results of audit tests are normally recorded by the auditors in checklists, along with evidence, notes and other documentation in the audit file.

Technical compliance tests may be necessary to verify that IT systems are configured in accordance with the organization’s information security policies, standards and guidelines. Automated configuration checking and vulnerability assessment tools may speed up the rate at which technical compliance checks are performed but potentially introduce their own security issues that need to be taken into account*.

The output of this phase is an accumulation of audit working papers and evidence in the audit files.

7.4 Audit analysis

The accumulated audit evidence is sorted out and filed, reviewed and examined in relation to the information risks and objectives or requirements, such as those in ISO/IEC 27001 and 27002 or other standards and references, and the audit scope and objectives. Preliminary findings, conclusions and recommendations may be drafted at this stage, concerning any significant issues identified.

Sometimes analysis identifies gaps in the evidence or indicates the need for additional audit tests, in which case further fieldwork may be performed unless scheduled time and resources have been exhausted. However, prioritizing audit activities by risk implies that the most important areas should have been covered already.

7.5 Audit reporting

Reporting is an important part of the audit process, and an involved sub-process all by itself.

A typical ISMS audit report contains the following elements, some of which may be split into appendices or separate documents:

- Title and introduction naming the organization and clarifying the scope, objectives, period of coverage and the nature, timing and extent of the audit work performed.
- An executive summary indicating the key audit findings, a brief analysis and commentary, and an overall conclusion, typically along the lines of “We find the ISMS compliant with ISO/IEC 27001 and worthy of

certification" or "Aside from [significant concerns], we are impressed with the coverage and effectiveness of the information security controls within the ISMS."

- The intended report lists out specific recipients (since the contents may be confidential) and contains appropriate document classification or instructions on circulation.
- An outline of the credentials, audit methods *etc*. of individual auditors and team members;
- Detailed audit findings and analysis, sometimes with extracts from the supporting evidence in the audit files where this aids comprehension.
- The audit conclusions and recommendations, perhaps initially presented as tentative proposals to be discussed with management and eventually incorporated as agreed action plans depending on local practices.
- A formal statement by the auditors of any reservations, qualifications, scope limitations or other caveats with respect to the audit.
- Depending on normal audit practices, management may be invited to provide a short commentary or formal response, accepting the results of the audit and committing to any agreed actions.

It is important that there is a factual basis meaning sufficient, appropriate audit evidence to support the findings reported. Audit's quality assurance processes should ensure that 'everything reportable is reported and everything reported is reportable', normally based on a review of the audit file by an experienced senior auditor. The wording of the draft audit report is checked to ensure readability, avoiding ambiguity and unsupported statements. When approved by audit management for circulation, the draft audit report is usually presented to and discussed with management. Further cycles of review and revision of the report may take place until it is finalized. Finalization typically involves management committing to the action plan.

Audit reporting is perhaps the one area where audit's formal independence is key. Auditors are *expected* to 'say what needs to be said'. However, given the aim to improve the ISMS and move the organization forward, it pays to express things very carefully … which takes experience, tact and time.

The auditor's assessment of the significance of any issues or shortcomings identified during the audit is the main determinant of a 'pass' or 'fail' result. Audit findings are commonly categorized according to their significance or severity, and (at least in respect of certification audits) reported as follows:

<u>Major Non-Conformance Report (NCR):</u> a nonconformity that **substantially affects the capability of the ISMS to achieve its objectives**. Nonconformities may be classified as major in the following circumstances:

- If there is significant doubt that effective process control is in place, or that the confidentiality, integrity and availability of information meets specified requirements; or
- A number of minor nonconformities associated with the same requirement or issue are symptoms indicative of a deeper and more substantial failure in the management system (*e.g*. poor governance).

Major NCRs are show-stoppers: in certification audits, they are likely to result in a refusal to issue or renew a compliance certificate unless the identified issues are resolved to the auditors' satisfaction.

<u>Minor NCR:</u> a nonconformity that **does not substantially affect the capability of the ISMS to achieve its objectives**. 'Substantiality' is a subjective matter for the auditor to determine, taking into account factors such as:

- The degree of departure from the recommendations in the ISO27k standards, or from generally accepted good practices in this domain;
- Whether the nonconformity is deliberate/intentional, or merely an oversight;

- The duration of the nonconformity - a complex issue this since sometimes longstanding issues are worth escalating to management's attention, yet the organization may have coped quite successfully with the nonconformity for the intervening period;
- The amount of information risk to the organization (by far the most important factor).

Observation or **O**pportunity **f**or **I**mprovement: a statement of fact based on and substantiated by objective evidence, identifying a weakness or potential deficiency in the ISMS which, if not resolved, the auditor believes may lead to nonconformity in the future.

According to convention and circumstances, the auditor *may* offer formal or informal recommendations, guidance and advice (*e.g*. promoting good practices and other improvements) but no specific solution need necessarily be provided. If an audit finding is expressed effectively and the issue is discrete, the resolution will often be self-evident. Ultimately, thanks to audit independence, it is the responsibility of management - not audit - to address the issues, acting in the best interests of the organization and taking account of other business priorities and objectives. Management must decide what to do and when to do it, if at all. In short, audits are merely advisory.

Even if they do not appear in formal audit reports, recommendations, observations and advice should normally be recorded on the audit file. Findings may be managed as identified risks, perhaps prompting follow-up work in future internal, surveillance or recertification audits and management reviews.

The output of this phase is a completed ISMS audit report, signed, dated and distributed according to the terms of the audit engagement letter.

7.6 Audit closure

In addition to indexing, cross-referencing and literally shutting the audit files, closure involves tidying up any loose ends, preparing notes for future ISMS or other audits, and perhaps following-up to check that the agreed actions are in fact completed more-or-less on time and as specified.

8. Competence and evaluation of auditors

8.1 Auditor competence

The following requirements apply to the audit team as a whole, or to the auditor if working alone. In each of the following areas of knowledge and expertise, at least one audit team member should take primary responsibility within the team:

- Managing the team, planning the audit, and audit quality assurance processes;
- Audit principles, methods and processes;
- Management systems in general and ISMS in particular;
- Relevant legislative, regulatory and contractual obligations applicable to the organization being audited;
- Information-related threats, vulnerabilities and incidents, particularly in relation to the organization being audited and comparable organizations, for example an appreciation of the likelihood of various types of information security incident affecting different forms of information, their severity and potential impacts, the controls typically used to mitigate the risks plus other risk treatment options such as cyber insurance;
- ISMS measurement techniques (information security metrics);

- Relevant ISMS standards, industry best practices, security policies and procedures;
- Business continuity management, including business impact assessment, incident management, resilience, recovery and contingency aspects;
- The application of information technology to business and hence the relevance of and need for cybersecurity; and
- Information risk management principles, methods and processes.

The audit team must be competent to trace concerns back to the relevant elements of the ISMS, implying that the auditors have appropriate work experience and practical expertise across the items noted above. This does not mean that every auditor needs the complete range of experience and competence in all aspects of information security, but the audit team as a whole should have a sufficiently broad range of experience and sufficiently deep competencies to cover the entire scope of the ISMS being audited.

In respect of ISMS audits, specifically, the auditors need to stay abreast of:

- The field: this is a dynamic area with frequent changes to the information risks (*i.e*. the threats, vulnerabilities and/or impacts), security controls and the cyber environment generally. It is therefore important that ISMS auditors maintain their knowledge of emerging and current threats, vulnerabilities being actively exploited, and the changing nature of incidents and impacts within the organization’s business context.
- Changes to ISO27k and other standards, guidelines *etc*.: aside from new and updated standards in the ISO/IEC 27000-series, there are frequent changes in other potentially relevant standards (*e.g.* the NIST SP800 series), guidelines and advisories (*e.g*. from ISACA).
- Legal and regulatory changes: GDPR (the EU’s General Data Protection Regulation) is a topical example of a significant forthcoming change to privacy laws and practices, with global business implications.
- Business and organizational changes: *e.g*. changing business activities, processes, priorities and relationships.
- Technology changes: *e.g.* new hardware, software and firmware; new paradigms such as IoT (**I**nternet **o**f **T**hings), BYOD (**B**ring **Y**our **O**wn **D**evice) and cloud computing.

8.2 Demonstration of auditor competence

Auditors must be able to demonstrate their knowledge and experience for example through:

- Holding recognized and relevant qualifications such as CISA;
- Registration as an auditor with a recognized professional body such as ISACA;
- Completion of recognized ISMS training courses such as “lead implementer” and “lead auditor”;
- Up-to-date continuous professional development records;
- Records confirming the audits in which they have participated (particularly ISMS and IT audits), and their roles; and/or
- Practical demonstration to more experienced auditors in the course of ISMS audits;
- Earning the trust and respect of colleagues.

Auditing is a highly privileged activity that depends on the auditees’ trust and respect, which must be *earned* by consistently high standards of professionalism, competence and personal integrity.

9. Document control

9.1 Authors

The following members of the ISO27k Forum updated this guideline in 2017: Bhushan Kaluvakolan; Richard Regalado; Gary Hinson and Pratibha Agrawal.

The following people contributed to the original 2012 version of the guideline: Alchap; Javier Cao Avellaneda; Anton Aylward; Pritam Bankar; Jesus Benitez; Lee Evans; Gary Hinson; Khawaja Faisal Javed; Lakshminarayanan; ; Rocky Lam; Prasad Pendse; Renato Aquilino Pujol; Bala Ramanan; Marappan Ramiah; Richard Regalado; Mninikhaya Qwabaza (Khaya); Kim Sassaman; Mooney Sherman; John South; Jasmina Trajkovski; Rob Whitcher and others.

9.2 History

March 2008 – First release of the guideline submitted to the ISO/IEC JTC1/SC27 committee via Standards New Zealand, and published as part of the free ISO27k Toolkit.

July-August 2017 - Entire document updated, first by a collaborative team effort using Google Docs and then finalized in MS Word, and republished in the ISO27k Toolkit.

9.3 Feedback

Comments, queries and (especially!) improvement suggestions are welcome either via the ISO27k Forum or direct to Gary Hinson (Gary@isect.com).

9.4 Copyright

Being a friendly and generous global community of ~3,500 ISMS professionals, the ISO27k Forum is an excellent source of further advice, support and guidance. ISO27001security.com offers information on the ISO27k standards, an FAQ and a toolkit.

Best of all, it's free!

Appendix A - Generic *information security* audit checklist

Introduction

The following checklist of audit tests is generic. It reflects and refers primarily to ISO/IEC 27002's advice on **information security controls** without regard to any *specific* control requirements that an individual organization might have in relation to its information risks identified through the risk assessment and risk management processes.

This is generic guidance to help review the organization's security controls, primarily against the recommendations in ISO/IEC 27001 Annex A, ISO/IEC 27002 and other ISO27k standards. It cannot provide specific guidance on the particular risks and controls applicable to every situation and must therefore be customized and interpreted by experienced IT auditors according to the context. For example, the organization's risk analysis may have determined that certain control objectives from the standards are not applicable and hence the corresponding controls may not be required, whereas in other areas the control objectives may be more rigorous than suggested in the standard and additional controls may be required. The **R**isk **T**reatment **P**lan and **S**tatement **o**f **A**pplicability should provide further details on this.

We have *deliberately* modified, extended or elaborated on the advice in ISO/IEC 27002 in various areas, based on our professional work and audit experience with ISMSs in various organizations and industries that take information security seriously (*e.g.* we have incorporated audit tests on business continuity). **This is not a simple compliance audit checklist.**

The audit tests noted below are intended as prompts or reminders of the main aspects that competent, qualified and experienced IT auditors would typically check. They do not cover every single aspect of information risk, security and related areas. They are not meant to be asked verbatim or checked-off piecemeal. They are not suitable for use by inexperienced auditors working without supervision.

The checklist is **not** intended to be used without due consideration and modification. ISMS auditors normally generate custom checklists reflecting the specific scope and scale of the particular ISMS being audited, taking into account any information security requirements that are already evident at this stage (such as information-security relevant laws, regulations and standards that are known to apply to similar organizations in the industry). Also, the audit checklist may be modified during the course of the audit if previously underappreciated areas of concern come to light. Finally, the checklist should reflect the auditors’ normal working practices, for example columns for audit notes, references to audit evidence on file, SWOT/PEST analyses of the findings *etc*.

Since completed ISMS audit checklists, files, notes and evidence contain sensitive information concerning the organization’s information risk and security arrangements, they *must* be adequately secured to ensure their confidentiality and integrity.

A.5. Information security policies

A.5.1 Management direction for information security

Numerous information security controls involve policies, hence policies appear many times in this checklist with audit tests reflecting various contexts and objectives. A.5.1.1 takes an overview of the entire policy suite.

A.5.1.1 Policies for information security: review the organization's policies for information risk, security and related areas (*e.g.* privacy, business continuity, compliance, governance, risk management, HR, physical/site security, change management, configuration management, incident management, logging, classification, systems development and acquisition …). Is there clear evidence of a sensibly designed and managed overall framework/structure/hierarchy? Are the policies reasonably comprehensive, covering all relevant information risks and control areas? How are the policies authorized, communicated, understood and accepted? Are all workers and where relevant their employers formally required to comply? Are there suitable compliance enforcement and reinforcement arrangements? Review the policies, standards, procedures, guidelines *etc*. for consistency with: good practices (such as ISO27k, NIST SP800 and other relevant standards, advisories and guidelines); applicable legal, regulatory and contractual obligations; corporate strategies and other policies. Are there appropriate cross-references, both internal and external? Are the policies well-written *i.e.* readable, reasonable and workable? Do they incorporate suitable and sufficient controls? Do they cover all essential information assets, systems, services *etc*.? How mature is the organization in this area? Look for issues (gaps, overlaps, inconsistencies/conflicts, poor quality writing, out-of-date/unapproved policies, missed review deadlines *etc*.) and opportunities for improvement.

A.5.1.2 Review of the policies for information security: evaluate the process for reviewing information security and related policies. Check a sample of policies for details such as: policy title; scope and applicability; status (*e.g.* draft, authorized, superseded, withdrawn); names of authors and accountable owners; version numbers; dates of publication; who approved them (*e.g.* Security Committee or an equivalent management body); document history/date of last and next reviews; associated compliance arrangements. Do all policies have a consistent format and style? Are they all current, having completed all due reviews (including feedback from ISMS management reviews and audits) and if appropriate been re-authorized and distributed? Cross-check evidence of approvals/authorization for a small sample. Look for issues and improvement opportunities.

A.6. Organisation of information security

A.6.1 Internal organisation

A.6.1.1 Information security roles and responsibilities: check the overall information risk and security governance and management structure. Is information risk and security given sufficient emphasis (is there a 'driving force'?) and management support? Is there a senior management forum to discuss information risk and security policies, risks and issues? Are roles and responsibilities clearly defined and assigned to suitably skilled individuals? Does each role have specific accountability towards information risk and security, relevant authority and are they competent (qualified) for the role? Is there sufficient budget for information risk and security activities? Is there coordination within the organisation between business units and HQ? Are the information flows (*e.g.* incident reporting) operating effectively in practice? Is there adequate awareness of and support for the information risk and security structure and governance arrangements?

A.6.1.2 Segregation of duties: check that operational duties or tasks that are critically important to information security have been identified, particularly those performed by information risk and security professionals plus IT personnel with elevated privileges on major information systems (servers, network devices, databases, applications *etc.*). Based on risk assessment, are duties segregated between roles or individuals where relevant *e.g.* to reduce the possibility of incompetence, negligence and inappropriate activities? Ideally a **RACI**-type matrix should be maintained identifying for each key task/duty who is **R**esponsible, **A**ccountable, **C**onsulted or kept **I**nformed, specifying for example that:

- Network and system administration should be separate from security administration;
- An access requester should not be able to approve his/her own requests, or be able to create his/her own login credentials;
- Access rights reconciliation should not be done *solely* by system administrators;
- Application developers and testers should not have routine access to production environments;
- Change requesters should not have the authority to approve their own requests;
- Reviews of firewall rules should not be done *solely* by network administrators;
- Security logs, incident reports, alarms and alerts should not be used and reviewed *solely* by IT professionals;
- Audits should be performed by competent, independent auditors.

Is there a policy covering segregation of duties? How are decisions regarding such segregation arrived at? Who has the authority to make such decisions? Are segregated duties reviewed periodically, when situations and risks change, or when incidents occur? Where segregation is impracticable or infeasible (*e.g.* a small organization), are compensating controls employed (*e.g.* additional logging or management oversight)? Is regular monitoring of activities and audit trails conducted? Is there adequate management supervision, especially for critical aspects (*e.g.* inexperienced, stressed or untrusted workers doing unfamiliar, complex and/or particularly important security work)?

A.6.1.3 Contact with authorities: is there readily available a list of contact details for regulatory or other authorities and bodies that might need to be contacted in case of queries, incidents and emergencies *e.g.* law enforcement, emergency services and maintenance/support personnel for HVAC, power, water supply, telecommunication services *etc.*? Check who is responsible for contacting the authorities and at what point of an incident / event is this contact made and how? Check if this has been done before and if informal and regular contact is maintained with these authorities so that the both sides (the enterprise and such authorities) are not surprised in times of emergency. Cross-check with the output of risk assessment if contact details for authorities for the identified significant risks are available. Is the list current and correct? Is there a maintenance process? (See also the compliance register in A.18.1.1).

A.6.1.4 Contact with special interest groups: is there regular or *ad hoc* contact with special interest groups, professional forums and mailing lists in information risk and security such as local chapters of ISACA, ISC^2, ISSA, ISO27k Forum *etc*.? Is information shared about emerging threats, new security technologies, good security practices, early warnings of alerts and advisories, newly discovered vulnerabilities and availability of patches *etc*.?

A.6.1.5 Information security in project management: review the information risk and security aspects of the organisation's project governance and management methods. Are information risks and security requirements identified and addressed at all stages of all projects, include all types of projects that concern information, new developments and changes/enhancements to existing systems, applications and processes? Does every project stage include appropriate activities? Do system/application/process/risk owners formally accept the residual risks (*e.g*. as part of final acceptance)?

A.6.2 Mobile devices and teleworking

A.6.2.1 Mobile device policy: review the policy and security controls relating to mobile and home users working on enterprise owned and issued *e.g.* corporate laptops, PDAs, Smartphones, iPads, tablets, USB/other mobile storage devices, VPNs *etc.* How are portable systems maintained and controlled (*e.g.* to ensure that they are kept up to date on antivirus definitions and security patches)? Confirm that all portable devices containing sensitive and proprietary corporate and personal data employ adequate access controls, normally implying installation of corporate images through MDM solutions, MAM solutions to control applications, whole-disk encryption, and rules around such access in case it is permitted.

6.2.2 Teleworking: review the policies, procedures, guidelines and practices relating to teleworking, remote and portable working. Check that information risks related to teleworking are determined, assessed and treated (*e.g.* suitable technical, physical and procedural security controls). Are security controls for teleworking equivalent to those for conventional office-type workplaces (any differences should reflect the respective information risks). Are there suitable arrangements for user authentication, network security, antivirus, backups, patching, security logging and monitoring, encryption, and business continuity? If required, how would the organization gain access to corporate or privately-owned ICT devices and media to confirm or configure their security, investigate incidents *etc.*?

A.7. Human resources security

A.7.1 Prior to employment

A.7.1.1 Screening: does the pre-employment screening process take into account relevant privacy and employment laws and regulations? Is this done in-house or contracted out to a third party? Are staff and contractors pre-screened prior to employment (including contacting references and a check of security clearance where appropriate)? If this is done by the third parties themselves, have their processes been reviewed and found acceptable? Are there enhanced screening processes for workers in particularly trusted roles (*e.g.* those with ROOT-equivalent access to sensitive systems), departments/functions, business units or sites? How is all this accomplished? There should be a documented consistent and repeatable process that is owned and maintained by HR and evidence should be available *e.g.* the results of such background checks. The attributes of such checks should be based on a risk assessment and conform to this control requirements, a risk acceptance of those requirements that cannot be met should be documented.

A.7.1.2 Terms and conditions of employment: are relevant information security roles and responsibilities adequately defined in job descriptions, offer letters, employment and service contracts, terms and conditions of employment *etc.* for information risk and security professionals, IT system/network managers, managers, auditors and workers in general? Are specific responsibilities relating to information risk and security identified, according to the nature of the roles? Check for suitable confidentiality and similar clauses (non-disclosure agreements). Are records maintained to prove that workers understood, acknowledged and accepted their information security obligations? Do (some) obligations continue for defined or indefinite periods beyond the end of employment?

A.7.2 During employment

A.7.2.1 Management responsibilities: review information security awareness, training and educational arrangements aimed at the management and supervisory audience. Are they regular and ongoing? Is the content and nature/format/style of awareness information and activities suited to the audience? Do managers receive appropriate awareness and training specifically on their key information risk and security-related roles and responsibilities (*e.g.* awareness of 'authorization' and 'oversight' in general, training in how to define and review access rights)? Are information risk, security and related activities and requirements (such as personal integrity and trustworthiness) identified in job descriptions, and are workers appropriately selected, trained and skilled? Does the induction program specifically cater for newly recruited or promoted managers providing important information and guidance on the organisation's information security posture, strategies, policies *etc*.?

A.7.2.2 Information security awareness, education and training: review the training of those specifically involved in operating the ISMS and the information security controls, and general information security awareness activities targeting all or specific groups of workers. Are necessary competencies and training/awareness requirements for information security professionals and others with specific roles and responsibilities explicitly identified? Is there a structured programme of initial (induction/orientation) and regular (ongoing/continuous) information security awareness and training for all types of worker? Is there a communications strategy or plan, typically involving leaflets and briefings, posters, emails, online learning management, quizzes, competitions, videos, social media (*e.g.* blogs) and other methods or activities on a sequence or range of topics? As well as specific topics, does the content cover more general aspects such as information risk, security and related concepts; management commitment and support; legal, regulatory, contractual and policy requirements; personal accountability and general responsibilities; contact points and further resources? Is the content updated or refreshed to reflect evolving information risks such as emerging threats, newly-identified vulnerabilities and recent incidents or near-misses, and changes such as new/revised policies? Are there periodic tests and exercises to check the level of awareness (if so, check the results including trends and any problem areas or concerns)? Are there follow up actions for any who do badly in such tests, and/or are changes made to the awareness and training materials?

> Continuous security awareness, training and education throughout the organization, top-to-bottom, helps build and maintain a **corporate security culture**: the traditional IT-focused 'end user security training' and 'annual security awareness updates' fall *well* short of good practice in this area.

A.7.2.3 Disciplinary process: do disciplinary processes cater for information security incidents, privacy breaches, piracy, hacking, fraud, industrial espionage *etc.* by workers? Review the policies, procedures, guidelines, practices and records arising. How are workers informed of the process, including the organization's expectations and their rights? Is this covered by contracts and agreements, induction training and ongoing awareness? Has the disciplinary process ever been invoked for information security incidents (if so, review recent cases; if not, why not)?

A.7.3 Termination and change of employment

A.7.3.1 Termination or change of employment responsibilities: review policies, standards, procedures, guidelines and associated records relating to information security for workers moving laterally or vertically within the organisation (*e.g.* promotions and demotions, changing roles, new responsibilities, new working practices *e.g.* teleworking) or leaving (resignations, planned or unplanned terminations). Evaluate the information risk and security aspects *e.g.* retrieving information assets (papers, data, systems), keys, removal of access rights, continued confidentiality of proprietary and personal information if required *etc*.

A.8. Asset management

A.8.1 Responsibility for assets

A.8.1.1 Inventory of assets: review any inventory of (information) assets, potentially covering:

- **Digital data**: business data of all kinds and all locations; IT/support data (*e.g.* configuration databases); passwords and biometrics; digital certificates and keys *etc.*;

- **Hardcopy information**: system and process documentation (covering specifications, architecture and design, installation, operation, use, management ...); licenses, agreements and contracts; awareness and training materials; business continuity management info, disaster recovery plans, exercises, reports *etc*.; other printed reports and logs (*e.g*. visitor books, facilities maintenance logs) *etc*.;
- **Software**: system software plus patches and vulnerability disclosures; applications, IT management utilities, databases and middleware, plus other packaged and bespoke software and patches; original installation media and/or hash-verified downloads; licenses; escrow arrangements *etc.*;
- **Infrastructure**: servers (physical and virtual, on- and off-site); network devices (routers, switches, load balancers, VPN devices, Web proxy servers); security devices (authentication servers, access control systems, gateways and firewalls, IDS/IPS, SIEM, spam and malware filters, logging and alerting systems); communication devices (modems, routers, leased lines, Internet connections, microwave links, WiFi Access Points); cables, patch panels, sockets and ports; end user devices (desktops and laptops, smartphones, tablets, BYOD devices); IoT *things*; SANs; back-up drives and tapes; filing cabinets, lockable enclosures, safes *etc*.;
- **Information services and service providers**: server, network, storage and backup, security, ICT support and other information-related operations and services; Internet and cloud services; Reuters, CERT and similar information feeds; third party operations, maintenance and support services *etc*.;
- **Physical security and safety**: smoke detectors, alarms and fire suppression systems; power provision including UPS and generators; air conditioning plus temperature monitoring and alarms; server racks, card access controls, perimeter fences, intruder alarms; fire safes on- and off-site; keys, especially master keys *etc*.;
- **Business relationships**: with external parties *e.g*. suppliers, partners, customers, advisors, regulators and authorities, owners and other stakeholders, particularly those involving the passage of information;
- **People**: in particular, any critical (more or less irreplaceable) or otherwise valuable individuals with unique knowledge, experience, skills, expertise or contacts, often performing vital roles.

Who owns the inventory? Review the associated management, administration and usage. How is the inventory maintained in a reasonably complete, accurate and up to date condition despite equipment/staff moves, new systems, business and IT changes *etc*. (*e.g*. a registration process for new systems)? Is it sufficiently detailed and appropriately structured? Look for both automated and manual inventory management processes (*e.g.* barcodes, security tags, procurement records, serial/MAC/EMEI numbers, stock-check/audit reports, network scans, links to other databases).

A.8.1.2 Ownership of assets: check that all critical information assets have appropriate accountable owners, and that their obligations (*e.g.* analysing and treating the associated information risks) are clearly defined for the entire lifecycle of the information. Check how ownership is assigned soon after critical assets are created or acquired. Check for evidence of this process happening on an ongoing basis. All assets must be appropriately tagged and asset tags and owners appropriately referenced in the asset register. Verify the organization's ownership/control of assets (*e.g.* if assets leased, what are the liabilities of both parties if there are information security incidents affecting them?).

A.8.1.3 Acceptable use of assets: is there a policy on acceptable use of technology resources such as email, instant messaging, FTP, responsibilities of users *etc*.? Does it cover user behaviour on the internet and social media. Is any personal use of enterprise assets allowed? If yes, to what extent and how is this monitored/ensured? Are DOs and DONTs and what constitutes improper use called out in any document? Is this circulated across the enterprise? Check whether an appropriate warning message or logon banner is presented to users that they must acknowledge to continue with the log-on process. Verify whether any monitoring procedures have been approved by legal counsel. Does the use of cryptography comply with all relevant laws, agreements/contracts and regulations?

A.8.1.4 Return of assets: how is this managed for all lateral movers and for those who have resigned or terminated. Is this an automated or manual procedure? If manual, how is it ensured that there are no slippages? Are all leavers mandated to hand over all enterprise issued assets before finally leaving, and how are any missing assets addressed?

A.8.2 Information classification

A.8.2.1 Classification of information: review policies, standards, procedures, guidelines and associated records relating to information classification. Is classification driven by government or defence obligations? Is classification based on confidentiality, integrity and/or availability requirements? Are the following aspects called out in the policy/procedure with respect to classified information: method of labelling, transfer, storage, handling removable media, disposal of electronic and physical media, disclosure, sharing, exchanging with third parties *etc.*? Are appropriate markings used on assets based on the classification of the information they contain? Classification is also needed for documents, forms, reports, screens, backup media, emails, file transfers *etc*. Are staff made aware of the corresponding security requirements for handling sensitive materials (*e.g.* no data that is classified as 'secret' to be generated, processed or stored on any system connected to the main corporate LAN/WAN or Internet)?

A.8.2.2 Labelling of information: is there a labelling procedure for information in both physical and electronic forms? Is it in sync with the information classification policy? How is correct labelling ensured? (How) does it link with the access control mechanism *e.g.* DRM? How is it ensured that only those with approved access permissions access information of relevant classification? And how is it ensured that there is no unauthorised access? Do asset owners review the classification levels at predefined intervals or in the instances of any significant change? Check that workers know what labels mean.

A.8.2.3 Handling of assets: further to A.8.2.1, check with respect to classified information belonging to or received from external sources: are their classification levels mapped appropriately to the organisation's own classification levels?

A.8.3 Media handling

A.8.3.1 Management of removable media: review relevant policy, procedure, standards, practices and records, in relation to the information risks. Is there an up-to-date and complete asset register for tapes, removable disk packs, CDs/DVDs, USB sticks and other removable media? Are removable media properly labelled, where required (*e.g.* classification and serial numbers) and accounted for in an asset register? Are archival media duplicated and verified prior to deletion of source data? Are archive tapes periodically verified and re-tensioned as per manufacturer's specifications (typically annually)? Are there appropriate controls to maintain confidentiality of stored data (*e.g.* encryption where required, limited access to tapes and drives, secure courier arrangements to transport high-risk media)? Are all media stored in a safe, secure environment as per manufacturers specifications? Are there authorisations for all media that need to be moved from one location to the other and are they accounted for at each stage?

A.8.3.2 Disposal of media: further to A.8.3.1, how are media disposed-of (in-house or outsourced to a third party - in which case has the third party been selected after due diligence and is there a suitable contract in place with the applicable security and assurance requirements)? Are there specific policy, contractual, legal or regulatory requirements for the disposal of media? Are there documented approvals at every stage for disposal of media? Are data that still need to be retained copied to other media and verified before such disposal? Are particularly sensitive data securely deleted prior to media disposal (*e.g.* by cryptographic erasure, degaussing and/or physical destruction)? Is documentary evidence retained of media destruction, and what is its retention period, review periods *etc.*? Do the arrangements include media embedded within equipment (*e.g.* multifunction devices)?

A.8.3.3 Physical media transfer: check the policy and procedure for control A.8.3.1. For media transported to other locations (*e.g*. backups stored offsite), check whether a reliable transport or courier is being used for the purpose. Check that a qualified individual identifies contents of media prior to transfer and if the contents are encrypted or not. Check that such transfer is recorded at every stage (hand over to transit custodians, leaving the initial facility/data centre, arriving at the destination, placed in storage *etc.*). Check that it is transported as per manufacturers specifications, appropriate protection applied during transfer, recording the times of transfer and receipt at the destination.

A.9 Access control

A.9.1 Business requirements of access control

A.9.1.1 Access control policy: review any access control and management policies, procedures, guidelines, practices and associated records. Are they consistent with the classification policy, joiners/movers/leavers procedures *etc*.? Is there appropriate segregation of duties? Is initial network/system access limited for new workers to get started (*e.g.* email and intranet only), subsequent access to business applications according to specific business needs being granted based on a defined workflow which includes approvals at appropriate levels?

A.9.1.2 Access to networks and network services: review the network services policy (may be part of a general access control policy). Besides standard requirements of access control to networks, how are VPN and wireless accesses authorised, controlled and monitored? Is multi-factor authentication in place for critical networks, systems and applications, especially for privileged users? How are networks monitored for unauthorised access, use or suspicious/anomalous activities? Are network security controls regularly checked and proven (*e.g*. penetration testing)? Does the organization measure and report incident identification and response times?

Since preventive controls are limited and competent hackers strive to conceal their activities, early detection and rapid response is generally considered a critical control.

A.9.2 User access management

A.9.2.1 User registration and de-registration: check for coverage in the access control policy and procedures. Are there unique user IDs for each user, generated based on a request workflow with appropriate approvals and records? Check that user IDs of leavers are disabled immediately based on a workflow. Are there effective links between Security Administration and HR plus Procurement for prompt notification when workers leave or move on? Is there a periodic review/audit to identify and suspend redundant user IDs? Are suspended IDs deleted after confirming that they are no longer needed? What prevents user IDs being reassigned to other users? If registration and de-registration is a manual process, check how an audit trail is maintained. Verify that the timing of de-registering an account is not counterproductive to the business (*e.g.* clients may send important information to an email account that was recently disabled; ownership of valuable business information may need to be reassigned from a redundant account to an appropriate active user).

A.9.2.2 User access provisioning: check that initial access for all users is basic (for example only email and intranet) and that all subsequent access to information systems and services is based on business needs. Check how it is ensured that all access that is granted conforms to the policies on access control and the segregation of duties. Beyond the basic access, there should be requests raised for all additional access with appropriate approvals at all stages till it is granted. Sample records for evidence that granted access rights are normally limited as far as practicable, and that access rights are regularly reviewed and if necessary promptly revoked (*e.g.* cross check a small sample against active accounts to ascertain whether all active accounts were properly authorized and only the authorised access was granted).

A.9.2.3 Management of privileged access rights: further to A 9.2.2, pay special attention to privileged users. Review system access/account controls for the users of privileged system, database, application and network managers' user IDs such as SYSTEM, Admin and ROOT. Verify that there are enhanced controls to reflect the greater potential for abuse of privileges *e.g.* special account authorisation procedures and monitoring systems to detect & respond to any such abuse. Is there a process in operation for more frequent and regular reviews of privileged accounts to identify and disable/delete redundant privileged accounts and/or reduce the privileges? Check the procedure for granting such elevated access and that separate user IDs are generated for granting elevated privileges. Has a time-bound expiry for privileged user IDs been set? Check the process for changing passwords or suspending user IDs as soon as possible when privileged users leave or moves internally. Are privileged user activities monitored even more closely in this period?

A.9.2.4 Management of secret authentication information of users: review user identification and authentication controls *e.g.* policies, standards, procedures, guidelines and technical controls such as minimum password length, complexity rules, forced change of passwords on first use, multi-factor authentication, biometrics, shared passwords *etc.* Evaluate the mix of technical/automated controls and manual procedures, management reviews *etc*. Does anyone routinely check for weak passwords and follow-up with user security awareness/training? Are new, replacement or temporary passwords provided to users only after confirming their identities? Is such information conveyed by secure means? Are generated or default passwords sufficiently strong *i.e.* not easily guessed or brute-forced? Are recipients required to acknowledge receipt of IDs and passwords? Are default vendor passwords changed immediately after installation of systems or software? Check the procedures and tools for temporary password generation: are they manual, semi- or fully-automated? Are users encouraged to use suitable password vault software (if so, is it sufficiently secure)? Confirm that passwords in systems/devices and applications are stored purely in encrypted form (preferably as salted hashes).

A.9.2.5 Review of user access rights: are periodic reviews of user access rights on systems and applications commissioned/requested by their 'owners' to check for changes in user roles such as promotions, internal moves and/or resignations? Are access rights and permissions adjusted or re-authorized accordingly? Is there a mechanism to ensure the reviews occur regularly, on time? Given the risks, are the access rights and permissions for privileged users reviewed more thoroughly and more frequently?

A.9.2.6 Removal or adjustment of access rights: check the procedure for removal or adjustment of access rights of employees, vendors and contractors on termination or change of their employment, contract or agreement. Does it include physical access to facilities and logical access to the network? Check if passwords of known or group user IDs (known to those who are leaving or moving internally) are changed when such departures or movements occur. In such cases, are departing / moving individuals removed from groups at the same time as changing passwords? Check a sample of records.

A.9.3 User responsibilities

A.9.3.1 Use of secret authentication information: check policy on the need to keep passwords, PIN codes *etc.*, confidential, not to divulge or record them, changing them promptly if compromise is suspected, and the need to have different passwords for various systems (including business *vs.* personal use). How is all this ensured? Explore the information risks and security controls relating to any shared accounts (*e.g.* are account owners held personally accountable for all activities under 'their' accounts, regardless of who actually uses them?).

A.9.4 System and application access control

A.9.4.1 Information access restriction: further to 9.2.2, review security designs and other documentation for a sample of major systems to determine whether suitable access controls are in place, including the use of individual user identities, user authentication, automated access controls, encryption *etc*. How are access rights, permissions and the associated rules defined, authorized, assigned, monitored/reviewed, managed and withdrawn?

A.9.4.2 Secure log-on procedures: are logon/user identification and authentication processes secured *e.g*. using the control-alt-delete key sequence to trigger a privileged kernel function? Are general warning notices displayed during log-on to dissuade unauthorised access, but not information which may help an unauthorised user identify and access the system/service? How are claimed user identities authenticated during the logon process? Has multi-factor authentication been implemented for critical systems/services/remote connections through VPNs *etc*.? Is logon information only validated after input is complete? Do invalid password trigger delays or lock-outs, log entries and alerts/alarms? Check also whether successful logons are being logged. Check that passwords are never transmitted over networks or links in cleartext.

A.9.4.3 Password management system: do systems enforce the password strength requirements laid down in corporate policies and standards? Do the rules define minimum password length, prevent reuse of a specified number of previously used passwords, enforce complexity rules (uppercase, lowercase, numerals, symbols, spaces *etc*.), forced change of passwords on first log-on, non-display of passwords as they are input, storage and (if necessary) transmission of passwords in encrypted form *etc*.?

A.9.4.4 Use of privileged utility programs: who controls privileged utilities? Who can access them, under what conditions and for what purposes? Check if these individuals have they been provided access based on a business need and an auditable approval process, and is each instance of their use logged? Confirm that access to any utility programs have not been made to users of applications or systems where segregation of duties is required.

A.9.4.5 Access control to program source code: check controls around program source code. Is it stored in one or more program source libraries or repositories, in secure environments with adequate access and version controls, monitoring, logging *etc.*? How is source code modified? How is code issued (checked out) and compiled? Are access and change logs stored and reviewed? Look for evidence.

A.10. Cryptography

10.1 Cryptographic controls

A.10.1.1 Policy on the use of cryptographic controls: is encryption required? If so, which information systems, networks, applications *etc*. does it cover? Is there a policy covering the use of cryptographic controls, covering the following:

- The general principles or circumstances under which information should be protected through cryptography;
- Standards to be applied for the effective implementation of cryptography;
- A risk-based process to determine and specify the protection required;
- Alignment with any documented requirements relating to IT equipment or services covered by contracts;
- Related security issues and trade-offs (*e.g*. the effects of encryption on content inspection for malware, information disclosure *etc*.);

- Adherence to applicable laws and regulations such as export restrictions (see A.18.1.1).

Check how all these requirements are satisfied and evaluate the residual information risks.

A.10.1.2 Key management: check that the cryptography policy covers the entire cradle-to-grave lifecycle of key management, including:

- Protection of equipment used to generate, store and archive cryptographic keys;
- Generating keys for different systems and applications;
- Sources of randomness, and avoidance of weak keys;
- Rules around changing/updating keys *e.g.* authorising, issuing, communicating and installing keys;
- Backing-up or archiving keys, recovering keys that are corrupted or lost, and destroying keys;
- Logging and auditing of key management activities;
- Handling official requests for access to cryptographic keys (*e.g.* court orders).

Check how all these requirements are satisfied and evaluate the residual information risks.

A.11. Physical and environmental security

A.11.1 Secure areas

A.11.1.1 Physical security perimeter: within the scope of the ISMS, are facilities reasonably discreet and sited to minimise disaster potential or cost of protective countermeasures (*e.g.* not adjacent to strife prone areas, in the flight path next to an airport *etc.*)? Check the defined security perimeters to sites, buildings, offices, computer and network rooms, network cabinets, archives, plant rooms, electrical switchgear *etc*. Are exterior roof, walls and flooring of solid construction? Are all external access points adequately protected against unauthorized access? Is the construction physically sound *e.g.* solid 'slab-to-slab' walls (extending past false floors and ceilings); strong, lockable doors and windows? Check whether all fire doors on the external perimeter wall are alarmed, cannot be opened from outside, are monitored by cameras, periodically tested and that they operate in a 'failsafe' manner. Confirm that only authorised personnel can enter the premises and how this is achieved. Check intruder detection systems, their periodic testing and evidence of this testing. Confirm that the controls comply with local or national standards and laws (*e.g.* building codes, health and safety rules).

> Health and safety of personnel may take precedence over information security *e.g.* protected emergency exit routes, 'crash bars' on outward-opening fire doors, fireman's override.

A.11.1.2 Physical entry controls: are suitable access control systems employed (*e.g.* proximity or card-swipe, security locks, CCTV monitoring, intruder detection) with matching procedures (*e.g.* key issue/return, regular access code changes, out-of-hours inspections by security guards, visitors routinely escorted and visits logged in room visitors book, material movement *etc.*)? Check for a physical security policy which covers all relevant areas such as issue of ID badges, visitor management, entry to defined areas of the building based on roles and responsibilities, access to the data centre(s), communication rooms and other critical areas *etc*. Are there procedures covering all these areas? If multi-factor authentication (*e.g.* biometric plus PIN code) is required for critical areas, check how this is implemented, functioning, monitored and administered. Check for access registers (*e.g.* visitor books) at data centres/IT rooms: is there a sound audit trail of all entries and exits? Check for a physical access review audit for the organisation, its method and periodicity.

A.11.1.3 Securing offices, rooms and facilities: are corporate facilities designed so that all access (ingress and egress) from the facilities is physically monitored and controlled (*e.g.* proximity detectors, CCTV surveillance). Ensure that corporate phone books and address directories are not readily available to all and sundry. Verify that the security controls used for securing offices, rooms and facilities are commensurate to the risks to the information assets stored, processed, or used in the said locations, with stronger controls for high-risk assets, rooms, areas *etc*.

A.11.1.4 Protecting against external and environmental threats: review protective controls against fire, smoke, flooding, lightning, intruders, vandals *etc.* Check the level of protection at disaster recovery, emergency and remote sites as well. See also A.11.2.

A.11.1.5 Working in secure areas: are supposedly vacated offices, IT rooms and other secure workplaces checked at end of day for both safety and security reasons? Are secure areas risk-assessed with suitable controls implemented, such as:

- Physical access controls;
- Intruder alarms;
- CCTV monitoring (check the retention and frequency of review);
- Photographic, video, audio or other recording equipment (including cameras and microphones in portable devices) prohibited; and
- Policies, procedures and guidelines.

How are details of proprietary business processes/activities in various areas of the facility kept confidential to authorised personnel?

A.11.1.6 Delivery and loading areas: are deliveries received and made in a secure area (*e.g.* access-controlled with only authorised personnel having access)? Is material received checked for safety and business reasons (*e.g.* an order number matching an authorized order)? Are details recorded as per procurement, asset management and security policies and procedures?

A.11.2 Equipment

A.11.2.1 Equipment siting and protection: is ICT and related equipment located in adequately protected areas? Are computer screens, printers and keyboards sited or protected to prevent unauthorised viewing? Check the controls to minimize the risk of physical and environmental threats such as:

- **Water/flooding:** facilities appropriately sited to minimize flood potential (*e.g.* above water table, not adjacent to water tanks, no water pipes overhead *etc*.). Where appropriate, additional/secondary protection installed and maintenance performed *e.g.* waterproof membranes, drip trays under air conditioning units, under-floor water detection with remote alarms and incident procedures, regular surveys or inspections of roofs, under-floor voids *etc.* for signs of water leakage/penetration;
- **Fire and smoke:** non-flammable facilities and fittings, fire alarms, low-smoke cabling *etc*.
- **Temperature, humidity and power**: see A.11.2.2
- **Dust:** equipment and air conditioner filters maintained (checked, cleaned, replaced) regularly. ICT facilities kept clean *e.g.* using specialist “deep cleaning" including floor and ceiling voids, low dust wall covering, under-floor sealed, dust covers/membranes *etc*. [Note: cleaners in sensitive areas such as computer rooms should normally be accompanied/supervised, unless cleaning is only done by competent, trustworthy staff. Cleaners may need to be security-cleared and proactively monitored if the organization handles government classified or other highly sensitive/valuable information.]
- **Lightning, static electricity and safety**: confirm that all exposed metalwork is earth bonded to a common safety earth point in accordance with electrical regulations. Confirm the use of mounted lightning conductors, cable isolators, fuses *etc.* where applicable. Are these controls tested periodically and following major changes?

- **Other:** *e.g.* theft, explosives, vibration, chemical contamination, electrical supply interference, communications interference, electromagnetic radiation and vandalism/criminal damage.

A.11.2.2 Supporting utilities - electrical power: check and ask Facilities or electrical engineers to explain the electrical power arrangements for computer rooms, network closets and other locations housing shared or critical IT systems (servers, PABX, communications hubs, security systems, safety systems, building management systems *etc*.). Are there computer-grade on-line UPSs, filters *etc*. providing reliable, high quality power? Is there adequate UPS capacity to support all essential equipment for a sufficient period (internal, rack-mounted, whole room or whole site systems)? How do we know that all essential equipment actually uses secure supplies? Are there generators of sufficient capacity? Are UPSs and generators operated, monitored and maintained as per manufacturer's specifications and tested *on-load* regularly? If appropriate, are there redundant (dual-routed) mains feeds from separate substations or grids? What happens when power cabling, switch gear or equipment changes or tests are made: are systems and services affected?

Air conditioning: are there properly specified and installed computer-grade air conditioners? Are chillers/condensers appropriately sited? Is there adequate A/C capacity to support the heat load, even in a hot summer? Are there redundant/spare units or portables available to improve resilience and permit maintenance without affecting service? Is there temperature sensing with remote-reading over-temperature alarms and incident procedures? Is air conditioning equipment professionally operated, tested and maintained as per manufacturer's specifications? Are there suitable operation and maintenance procedures, including filter cleaning and dealing with over-temperature or other alarms?

Other: check if the facilities and supporting utilities (*e.g*. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) are being inspected and tested regularly to ensure their proper functioning. They should be alarmed for malfunctioning, and perhaps for unauthorized activity. Check how alarms are handled out-of-hours (*e.g*. do security guards have remote alarm indicators/sounders on their consoles, with suitable response procedures, training/exercises *etc*.?).

A.11.2.3 Cabling security: is there appropriate physical protection for external cables, junction boxes, air conditioner chillers, microwave dishes, air inlets *etc.* against accidental damage or deliberate interference? Check whether the power cables are segregated from communications cables to prevent interference. Check whether access to patch panels and cable rooms is controlled, with cabling concealed/protected against eavesdropping by attaching rogue devices, or physical damage. Are there suitable procedures to confirm all this? Verify that cabling installations are done in accordance with building codes and other applicable regulations, standards and policies.

A.11.2.4 Equipment maintenance: check that only qualified personnel carry out maintenance of equipment (infrastructure and network devices, laptops, desktops *etc*. and all safety and utility equipment such as smoke detectors, fire suppression devices, HVAC, access control, CCTV *etc*.), check that equipment is maintained and serviced according to the manufacturers' specifications. Are there up-to-date maintenance schedules and logs/reports? If equipment is insured, are maintenance and other requirements of the insurance contract satisfied?

A.11.2.5 Removal of assets: check the policy and procedure concerning removal of information assets (ICT equipment, storage media and the information content) from sites, buildings, offices, archives and other locations. Are there documented approvals or authorizations at appropriate levels (*e.g.* equipment or information owners)? [How] are movements restricted to authorised personnel? What stops people secreting USB drives and other small storage devices about their person? Check the procedures for tracking movements of high-value or high-risk assets. Walk through the process. Check a sample of records pertaining to movements for accuracy and completeness.

A.11.2.6 Security of equipment and assets off-premises: is there an 'Acceptable Use Policy' or equivalent guidance covering security requirements and 'DOs and DONTs' for all mobile or portable devices that are used from home or remote locations? Does it state requirements such as appropriate custody and secure storage, physical and/or logical access control (*e.g.* lockable cabinets, encryption), secure connections (*e.g.* VPNs), clear desks and clear screens, protection from strong electromagnetic fields, regular backups *etc*. How is all this achieved and ensured in practice? How are workers made aware of their obligations? Are they given enough support to achieve an acceptable level of security?

A.11.2.7 Secure disposal or re-use of equipment: review policies, standards, procedures, guidelines and associated records relating to how storage media and ICT equipment are re-used or disposed-of. How does the organization prevent stored information being disclosed, to a sufficient assurance level given the associated information risks (*e.g.* relating to the data or system classification)? If there is a reliance on strong encryption or secure erasure, how does that work and how are non-functional devices and media disposed-of? Are suitable records maintained of all media that are disposed-of, with details such as nature of contents, form of disposal and where appropriate positive confirmation of secure disposal? Does the policy and process cover *all* ICT devices and media? Hunt for exceptions.

A.11.2.8 Unattended user equipment: if active user sessions are suspended or terminated after a defined idle time, how are applications suspended/terminated to avoid data loss or corruption? Is the idle time definition appropriate, given the risks of unauthorized physical access to active/logged-on devices? If screen-locks are used, are they password-protected? Does this policy apply to *all* servers, desktops, laptops, smartphones and other ICT devices? How is it checked and enforced? Are any exceptions risk-assessed and authorized by management as policy exemptions?

A.11.2.9 Clear desk and clear screen policy: review policies, standards, procedures and guidelines in this area. How well is it working out in practice? Walk around checking for insecure information assets such as logged-on but unlocked servers, PCs, laptops and smartphones, insecure digital storage media (such as USB memory sticks) and paperwork (*e.g.* diaries; passwords on Post-It notes; files, forms and notes containing sensitive business or personal information; printouts abandoned on printers and copiers; unlocked filing cabinets). Do all computing devices have a password-protected screen saver or lock which employees use when stepping away from their devices, or that it kicks in after a defined idle time? Check the procedures around usage of printers, photocopiers, scanners, cameras and any other reproduction technologies.

A.12. Operations security

A.12.1 Operational procedures and responsibilities

A.12.1.1 Documented operating procedures: review the general state of procedures for IT operations, systems and network management, incident management, IT security administration, IT and physical security operations, change management *etc*. Is there a full set of security procedures in place and when were they last reviewed? Are the processes reasonably secure and well-controlled? Are information security aspects appropriately included (*e.g.* incompatible duties segregated to separate staff, incident notification procedures, management oversight *etc*.)? Are corresponding responsibilities clearly assigned to roles and hence to individuals, along with training, exercises *etc*.? Areas which typically require documented management and/or operational procedures include: change, configuration, release, capacity, performance, problem, incident, backups and archives (including storage and restoration), media handling, logs and audit trails, alarms and alerts, operational security (*e.g.* hardening, vulnerability assessments, patching, antivirus configuration and updates, encryption *etc*.). Look for evidence confirming that the procedures are being routinely reviewed and maintained, authorized/mandated, circulated and used. Sample and assess high-risk or known problematic procedures more thoroughly.

A.12.1.2 Change management: review non-IT change management policies, procedures, standards, practices and related records. Are changes planned and managed, impacts assessed (taking account of information risk and security aspects, plus the impacts of *not* changing!). Review a small sample of change management records, focusing on high-risk changes. Are changes properly documented, justified and authorized by management? Look for improvement opportunities. (See also A.14.2.2).

A.12.1.3 Capacity management: review capacity management policies, procedures, practices and associated records. Does it include aspects such as: defined service levels, monitoring of relevant metrics (*e.g*. server CPU usage, storage space and hard page faults, network capacity, power demand and air conditioning capacity, rack space, utilization and stress rates for key workers), alarms/alerts at critical levels, forward planning (taking account of procurement lead times and change management) *etc*.? Is there evidence of a risk-based approach *e.g.* a priority on ensuring the performance and availability of critical services, servers, infrastructure, applications, functions *etc*.?

Cross-check against **B**usiness **C**ontinuity **M**anagement (*e.g*. BCM business impact assessments systematically identify information and supporting services that are critical to the business).

A.12.1.4 Separation of development, testing and operational environments: review policies, procedures, practices, associated records and architectures that separate or segregate development, testing and operational ICT environments (including quality assurance/quality control, pre-production, dual-live/mirrored, load-balancing, failover and disaster recovery configurations, plus dynamic resource allocations in the cloud). How is separation achieved to an adequate assurance level (according to the risks)? Check for adequate controls isolating each environment (*e.g.* production/business networks segregated from other networks used for development, testing, management including security, logging, monitoring and alerting). Check access controls for these environments. Confirm (by enquiry and sample testing) that only authorised workers have access through appropriately differentiated user profiles to each of these environments. How is software promoted and released? Review evidence of approval of requests prior to granting access, and periodic access reviews. Check that change management applies to the authorization and migration of software, data, metadata and configurations between environments in either direction (*e.g*. production data copied into development or test environments). Consider the information risk and security aspects including compliance (*e.g*. privacy implications if personal data are moved to less secure environments or outside the EU). Who is responsible for ensuring that new/changed software does not disrupt the infrastructure, other systems, networks and operations *etc*.?

A.12.2 Protection from malware

A.12.2.1 Controls against malware: review malware policies, procedures, guidelines, practices and associated records. Check any white-list or black-list of applications that can or cannot be used in the enterprise. How is the list compiled, managed and maintained, and by whom? Review malware protection and incident response procedures and a sample of malware incident reports. Are there continuous/frequent virus-checks on all relevant devices including standalones, portables, embedded devices and IoT *things*? Are infection levels minimised (*i.e.* is the situation broadly under control)? How is anti-virus software updated, both manually and automatically? Is malware detected by scanners reported to an appropriate co-ordinator? If notification is manual, roughly what proportion gets notified (all, most, some or just a few)? Is there adequate protection against ransomware, Trojans, worms, spyware, rootkits, keyloggers, **A**dvanced **P**ersistent **T**hreats *etc*.? How are technical vulnerabilities managed? Is there appropriate ongoing training and awareness covering detection, reporting and resolution of malware for users, managers and support specialists? In the event of a serious incident, check the associated controls to investigate and resolve the incident, including rapid detection of outbreaks and network isolation, escalation to management, notification of affected parties, invocation of business continuity arrangements, forensic analysis *etc*.

A.12.3 Backup

A.12.3.1 Information backup: review backup policies, procedures, practices and associated records. Is there a risk-based mandate for an accurate and complete record of backups whose extent and frequency reflect business requirements? Do backup strategies cover data and metadata, system and application programs including utilities, configuration parameters *etc*. for all systems including servers, desktops, phone/network systems, system/network management systems, standalone/portable systems, control systems, security systems *etc*.? Are backup media physically protected/secured to at least the same level as for operational data? Are backups stored in suitable diverse locations, guarding against physical disasters, fires, thefts *etc*.? Are backups regularly tested to ensure they can in fact be restored intact? Are archives explicitly designed long-term secure, diverse, assured storage and restoration (*e.g*. archive media *and* devices)? Check that any defined recovery time and point objectives can be met. Using a small sample, check whether backup media listed in the records actually exist in the right place and are properly secured and labelled. Check any technical and management reviews in this area, including findings and actions arising. Assess the associated information risks (confidentiality, integrity *and* availability aspects).

A.12.4 Logging and monitoring

A.12.4.1 Event logging: review event logging policies, procedures, practices and associated records. Are *all* key systems (including event logging itself) being monitored and logged consistently and securely? What events or parameters are being monitored (look for evidence of an architecture, design or structured database)? Check for logging of security-relevant events such as: changes to user IDs, permissions and access controls; privileged system activities; successful and unsuccessful access attempts including logon and logoff; device identities and locations, plus network addresses and protocols; software installation and changes to system configurations (*e.g*. clock resets, log stop/start, alarm cancel); use of system utilities and applications; files accessed and the kind of access). Check by sampling that security incidents are being duly reported, assessed and resolved. Who is responsible for reviewing and following-up on reported events? How long are event logs *etc*. retained? Is there a process in place for reviewing and responding appropriately to security alerts from vendors, CERTs, professional interest groups, government sources *etc*.? Is the overall process running reasonably well in practice? How could it be improved?

A.12.4.2 Protection of log information: where appropriate, are logs being stored/archived in a non-editable secure format or control mechanism? Is access to logs adequately controlled, authorized and monitored? Who has, or might obtain, read/write/delete access to event logs, and is that appropriate? Is there sufficient storage capacity given the average volume of logs being generated and the retention requirements (duration)? Check the historical status of these requirements.

A.12.4.3 Administrator and operator logs: review policies, procedures, practices and associated records concerning privileged administrators, operators *etc*. including security, SIEM and outsourced service administrators. How are the logs collected, stored and secured, analysed/monitored and maintained (*e.g*. archived for later forensic analysis)? Where appropriate, do the security arrangements limit the ability of such individuals to interfere with the logs or the logging arrangements, at least not without raising security alarms and incidents? Consider the risks and identify any issues or opportunities for improvement.

A.12.4.4 Clock synchronisation: review policies, architectures, procedures, practices, guidelines and associated records concerning system clock synchronization and accuracy. Is there a defined reference time (preferably based on atomic clocks *e.g.* GPS or NTP to a stratum 1 time reference)? Does the method for synchronising clocks with the reference meet business, security, operational, legal, regulatory and contractual requirements? Has this been implemented across the IT estate including monitoring systems such as CCTVs, alerting and alarm systems, access control mechanisms, auditing and logging systems, IoT *things etc*.? Check the monitoring arrangements. What actually happens if a time reference becomes unavailable for some reason? Have the associated information risks been analysed and appropriately treated? How are clock changes, leap seconds *etc*. handled?

A.12.5 Control of operational software

A.12.5.1 Installation of software on operational systems: review policies, procedures, practices and associated records concerning software installation. Check that only fully tested, approved and currently supported/maintained software is installed for production use. Hunt down any outdated and especially no longer supported/maintained software on productions systems (firmware, operating systems, middleware, applications and utilities). Check that desktops, laptops, servers, databases *etc*. are configured to prevent software installation except by trained and authorized administrators under management authority. Do the management and monitoring systems and practices flag-up any unapproved software installations, reporting them to and recording them on the configuration management database, monitoring/alerting systems *etc*.? Cross-check against change and configuration management, security management, business continuity and other relevant areas, focusing on high-risk/critical systems.

A.12.6 Technical vulnerability management

A.12.6.1 Management of technical vulnerabilities: review policies, procedures, practices and associated records concerning the management (identification, risk-evaluation and treatment) of technical vulnerabilities. How does the organization discover and respond to technical vulnerabilities in desktops, servers, applications, network devices and other components? Review incident and change control records for evidence relating to recent patches, vulnerability assessments, penetration testing *etc*. Are there suitable processes in place to check systems inventories and identify whether disclosed vulnerabilities are relevant? Has a comprehensive risk assessment of ICT systems been performed? Have risks been identified and appropriately treated, prioritized according to risk? Is risk assessment ongoing to identify changes such as emerging threats, known or suspected vulnerabilities, and evolving business impacts or consequences? Are patches assessed for applicability and risks before being implemented? Are the processes for implementing urgent patches sufficiently slick and comprehensive? To what extent does the organization depend on automated patch management, in effect accepting the associated risks of implementing rogue patches? Look for any evidence of important systems that have not been maintained at current release levels and/or patched against known vulnerabilities.

A.12.6.2 Restrictions on software installation: check that only authorised personnel having appropriate system privileges are able to install software on systems. Check how many categories of such privileges are there and what privileges each category has. Check what types of software each of these categories can install, on which systems. Do the controls apply to patching, backup restores and online downloads as well as conventional system installations?

A.12.7 Information systems audit considerations

A.12.7.1 Information systems audit controls: check that information security audits are a policy requirement. Is there a defined program and procedure for audits? Verify whether audit requirements involving checks on operational systems are carefully planned and agreed to minimise the risk of disruptions to business process. Verify whether the audit scope is agreed to with appropriate management. Verify that access to information system audit tools/software is controlled to prevent misuse and compromise. Verify the segregation of system audit tools from development and operational systems, and that they are provided an appropriate level of protection.

A.13. Communications security

A.13.1 Network security management

A.13.1.1 Network controls: check if there is a policy covering both wired and wireless networks. Is management of computer operations separate from network operations? Check for adequate security protection mechanisms on the networks. Check for appropriate logging and monitoring of the network and its devices, check for 'fail-proof' authentication procedures for all access to the organisations network. Check how network access points are secured against unauthorized access? How does the system limit access by authorized individuals to legitimate applications/services? Are users authenticated appropriately at logon (including dial-in and remote/Web users)? How are network nodes authenticated? Are distinct security domains established using firewalls, VLANs, VPNs *etc*.? Confirm protection of any privileged system management and remote support ports *e.g.* secure modems, challenge-response systems, key lock-out *etc*.

A.13.1.2 Security of network services: check for a policy on the following and how they are implemented in day-to-day operations:

- Secure management of information services;
- Monitoring of network services;
- Right to audit as part of contract in case of managed network services by a third party (contracts, SLAs and management reporting requirements);
- Authentication on the network, plus encryption and network connection controls;
- Periodic review of technical parameters, firewall rule review, IDS/IPS signatures *etc*.

A.13.1.3 Segregation in network services: check the policy on network segregation and consider the risks. What types of network segregation are in place? Is network segregation based on classification, trust levels, domains (public, desktops, servers, functions), a combination or something else? Check how segregation is achieved, monitored and controlled. How are wireless networks segregated from wired networks? Check how guest networks are segregated from corporate networks. Are there adequate controls between them? If there are any extranets with vendors *etc*., how are these secured? Is the security adequate given the risks and the risk appetite of the enterprise?

A.13.2 Information transfer

A.13.2.1 Information transfer policies and procedures: check for a policy on the subject and for procedures around secure transmission of information via email, FTP and other data transfer applications and protocols, Web (*e.g.* groups/forums), Dropbox and similar cloud services, WiFi and Bluetooth, CD/DVD, USB stick, courier *etc*. Check how various categories (classification levels) of information are required to be secured when transferred. Are access controls adequate? Where, when and how is cryptography mandated (*e.g.* link encryption, email encryption, encrypted ZIPs)? Check that suitable confidentiality or privacy arrangements (such as **N**on-**D**isclosure **A**greements, identification and authentication, out-of-band disclosure of encryption keys, non-repudiation/proof of receipt) are in place prior to the exchange of sensitive or valuable information. Check the associated awareness, training and compliance arrangements too.

A.13.2.2 Agreements on information transfer: further to A.13.2.1, on what types of communications are digital signatures implemented? Check liabilities and control in case of data loss, corruption, disclosure *etc*. Check identification and synchronisation of information classification levels of all involved parties. How is a chain of custody maintained for data transfers?

A.13.2.3 Electronic messaging: check for policy on control requirements around email, review policies and procedures for data exchanges *e.g.* communications network links including email and FTP/SFTP, dial-up links *etc*. Are there suitable security controls (*e.g.* email/link encryption, authentication and non-repudiation based on message classification *etc*.)? Review security arrangements for Internet, Intranet and related systems (bulletin boards *etc*.).

A.13.2.4 Confidentiality or non-disclosure agreements: locate and check the content of any such agreements. Have they been reviewed and approved by Legal? When were they last reviewed (periodic or change-driven)? Have they been approved and signed by the appropriate people? Are there suitable penalties and expected actions in case of noncompliance and/or benefits for compliance (*e.g*. a performance bonus)?

A.14. System acquisition, development and maintenance

A.14.1 Security requirements of information systems

A.14.1.1 Information security requirements analysis and specifications: check the policy, procedures, guidelines, practices and records in this area. Are formal systems development methods used routinely for high-risk systems *e.g*. safety-, business- or mission-critical? Are information risk analysis, functional and technical requirement specification, security architecture/design, security testing and certification *etc*. mandatory activities for all new developments and changes to existing systems (*e.g*. maintenance updates, operating system/application upgrades, crypto changes *etc*.). Are information risks handled in a similar way for commercial systems and software including bespoke, custom and off-the-shelf products?

A.14.1.2 Securing application services on public networks: if the organization uses or provides web based applications or other eCommerce systems, review the corresponding information security controls for access and user authentication, data integrity and service availability. Review security designs for a small sample of major systems to determine whether controls such as input data validation, processing validation, encryption, message authentication, non-repudiation *etc.* are employed appropriately. Check for the enforced use of https, for example, to protect sensitive data *en route* between Web browser and server. Review system security documentation. Are such requirements covered by policy? If the organisation subscribes to a 'threat intelligence’ service, check which public websites are being monitored. Are identified threats being routinely documented, risk-assessed and treated through incident and change management procedures?

A.14.1.3 Protecting application services transactions: further to A.14.1.2, check how transaction integrity, confidentiality, availability and prevention of mis-routing are achieved. Are transactions performed and stored in a secure internal environment (not open to the Internet!)? Do they meet all jurisdictional legal, regulatory and compliance requirements?

A.14.2 Security in development and support processes

A.14.2.1 Secure development policy: is there a policy on secure development covering security architectures, services and software? Are development environments and repositories secure with access control, security and change monitoring *etc.*? Do development methods include secure coding guidelines? Confirm that developers have adequate knowledge about secure coding practices and are capable of using secure programming techniques in instances of code re-use where development standards may not be fully known. These checks are to be performed even if development is outsourced to third parties.

A.14.2.2 System change control procedures: review IT system change management policies, procedures, standards, practices and related records. Do they include planning and testing of changes, impact assessments (including information risk and security aspects, plus the impacts of *not* changing!), installation verification checks and fall-back/back-out/reversion procedures (tested!), both standard (production and non-production) and emergency changes *etc*.? Do they cover significant changes to computing and telecommunications equipment (hardware), key system and security parameters, system and application software, firmware *etc*.? Review a small sample of system change management records, focusing on high-risk system changes. Are system changes properly documented, justified and authorized by management? Look for improvement opportunities. (See also A.12.1.2).

A.14.2.3 Technical review of applications after operating platform changes: assess whether changes to systems (*e.g*. maintenance updates, operating system/application upgrades and patches, crypto changes *etc*.) trigger security reviews/risk assessments and, if necessary, re-certification of systems. Confirm that this has been done on a sample of systems.

A.14.2.4 Restrictions on changes to software packages: check if changes have been made to software packages, confirming that original built-in controls have not been compromised. Was vendor consent and involvement obtained? Does the vendor support continue? Was the possibility of getting standard program updates from vendors explored? Was compatibility checked with other software in use?

A.14.2.5 Secure system engineering principles: confirm that secure system engineering principles have been documented and incorporated within the project governance framework/methods. Check security aspects of the SDLC process which should have sections and steps to check for security controls, check for endorsement from top management for all projects to follow the secure SDLC process, check if Developers and Programmers are trained on secure software development, check for evidence of stage/phase/toll gate checks which include security checks and approvals for all development and enhancement projects.

A.14.2.6 Secure development environment: review the controls isolating development from testing and production environments. How is software developed, tested and released? Who is responsible for ensuring that new/changed software does not disrupt other operations? Confirm if background checks have been performed of developers and that they are mandated to abide by the NDA. What are the applicable regulations and compliance requirements affecting development? How are test data derived and protected against disclosure and where are they stored? Check for evidence or steps which include security checks and approvals of software code before being released.

A.14.2.7 Outsourced development: further to A.14.2.6, check:

- Licensing arrangements, code ownership and intellectual property rights related to the outsourced content;
- Contractual requirements for secure design, coding and testing practices *e.g.* secure development methods; protection of specifications, designs, test data, test cases and test results;
- Escrow arrangements *e.g.* access to source code if executable code needs to be modified but the supplier is no longer available or capable;
- Application security testing controls and the test results;
- Vulnerability assessment and mitigation.

A.14.2.8 System security testing: check for a thorough testing and verification procedure for all new and updated systems which include a detailed schedule of activities, test inputs and outputs under a range of conditions. Check licensing arrangements, code ownership and intellectual property rights related to the outsourced content.

A.14.2.9 System acceptance testing: how are acceptance tests (including IT security aspects) completed prior to the introduction of new systems onto the network? Evaluate in conjunction with A.14.1.1, A.14.1.2 and A.14.2.1. Is testing automated, manual or both? Do tests replicate realistic operational environments and situations? Are security-related defects remediated before product are certified/passed? Is there user acceptance testing before release to the operational environment? Check whether fault-tolerant or redundant information systems, failover mechanisms, disaster recovery arrangements *etc*. are regularly tested to ensure they work as intended. Are resilience and recovery controls updated to reflect new, changed and retired systems?

A.14.3 Test data

A.14.3.1 Protection of test data: confirm that testing systems have appropriate access control. Check what data is used for testing and how it is protected. If operational ('production') data is used for testing, confirm that there is an appropriate approval process for use of this data before it is acquired for testing (especially if it contains personal information or other sensitive content), check if such data is adequately masked before use, and that it is erased immediately after testing. There should be audit logs when operational data is being copied for testing and these should be archived.

A.15. Supplier relationships

A.15.1 Information security in supplier relationships

A.15.1.1 Information security policy for supplier relationships: review the policies, processes, practices and records relating to the management of supplier relationships involving outsourced IT and cloud, logistics, utilities, HR, medical, financial, legal and other services with significant information risk, security or compliance implications. Where applicable, do contracts and agreements adequately address:

- Relationship management arrangements including the information risk and security aspects, metrics, performance, issues, escalation routes *etc*.;
- Information/intellectual property ownership, and obligations/constraints arising;
- Accountability and responsibilities relating to information risk and security;
- Legal, regulatory and policy requirements, such as certified compliance with ISO/IEC 27001;
- Identification of and protection against information risks using physical, logical/technical procedural/manual and legal/commercial controls (some of which may be specified *e.g*. collaborative risk management);
- Handling of events, incidents and disasters including evaluation, classification, prioritization, notification, escalation, response management and business continuity aspects;
- Security clearance of employees, plus awareness, training *etc*. (by either or both parties);
- A right of [security] audit by the organisation and/or whistleblowing mechanisms?

Is either party contractually bound to abide by [some of] the other's information risk, security or related policies in addition to their own, and how are any conflicts addressed? Are external service providers *routinely* monitored and (if applicable) audited for compliance with security requirements, or only in response to identified incidents or issues? How are any changes in the associated information risks identified and responded to? Evaluate the available evidence.

A.15.1.2 Addressing security within supplier agreements: if applicable, check for formal contracts or agreements with suppliers covering the following:

- Relationship management including information risk and security management, coordination, reporting, metrics *etc*.;
- Comprehensive and binding non-disclosure agreement or clauses;
- Description of information that will be handled, methods of accessing the information;
- Information classification scheme that must be followed;

- Applicable policy, legal and regulatory compliance requirements, plus any obligation to implement specific controls (*e.g*. access controls, performance reviews, monitoring, reporting, auditing);
- Prompt information security incident notification/escalation and collaboration during incident management and resolution;
- Business continuity aspects such as no-fault resolution, best endeavours, alternative sources, escrow;
- Sub-contracting and constraints on relationships with other suppliers, customers, partners and competitors;
- Personnel and HR aspects *e.g*. handling performance issues or trust concerns, no poaching our best people!

Check that the associated security and compliance aspects are covered during periodic relationship management meetings *etc*.

A.15.1.3 Information and communication technology supply chain: further to A.15.1.1 and A.15.1.2, check how information risk and security practices propagate throughout the supply chain, especially when parts are subcontracted. How are the security requirements of acquired products (goods and services) validated? How is resilience achieved where critical products or services are supplied by others? Can their origin be traced if needed (*e.g*. firmware and embedded systems)?

A.15.2 Supplier service delivery management

A.15.2.1 Monitoring and review of supplier services: how are services monitored and who is responsible for this activity? Are service review meetings conducted, at what frequency and with what audiences? Check security-related reports, presentations and metrics reviewed and decisions made at such meetings. Are information risks, incidents, policies, compliance, management review and audit reports *etc*. discussed during these meetings? Are there penalty or bonus clauses in the contract concerning information risk and security requirements, and how well are they working in practice?

A.15.2.2 Managing changes to supplier services: what happens if there are any changes to information-related services provided, such as additional services or changes to the way contracted services are delivered? Also if the organization’s security policies, standards or laws and regulations change, and suppliers are required to comply with them. How are such situations handled in practice? Look for examples.

A.16. Information security incident management

A.16.1 Management of information security incidents and improvements

A.16.1.1 Responsibilities and procedures: review the policy, procedures, guidelines *etc*. on incident management covering:

- Incident response planning and preparations;
- Nominated point/s of contact for incident reporting, tracking and feedback (*e.g*. status updates);
- Monitoring/detecting and reporting information security events;
- Analysing, evaluating and where appropriate assigning events to resolving agencies, incident response teams *etc*.;
- Escalation paths including emergency responses, business continuity invocation *etc*.;
- Planned methods of collecting digital forensic evidence where needed;
- Periodic and/or post-event security review meetings and learning/improvement processes *etc*.

Check a sample of records arising from incident reporting, logging, triage, assignment to resolution agencies, mitigation, confirmation of closure, learning points *etc*. Look for issues and improvement opportunities.

A.16.1.2 Reporting information security events: how are information security events (plus incidents, near-misses and weaknesses) reported *e.g.* phone call, email or SMS text to Help/Service Desk; incident reporting app or form on the intranet; in person report to information security/line manager *etc.*? Are workers aware of the need to report promptly, and do they do so routinely in fact (check the metrics!)? What happens to such reports? Trace the information and workflow using relevant records, archived incidents *etc*. comparing what actually happened against policies, procedures and guidelines. Speak with people who have recently reported events to explore the experience and outcome from their perspectives.

A.16.1.3 Reporting information security weaknesses: further to A.16.1.2, check that workers are mandated (and encouraged through awareness and training, and enabled through reporting mechanisms) to report any kind of unusual occurrence such as systems and applications logging in or logging out automatically, unprogrammed session timeouts, phishing or spam emails, or any other noticed or suspected and unusual occurrence. Do the policies explicitly prohibit workers from 'checking', 'exploring', 'validating' or 'confirming' vulnerabilities unless they are *expressly* authorized to do so?

A.16.1.4 Assessment of and decisions on information security events: check what is expected of all employees as far as reporting information security events and incidents are concerned. What exactly are they expected to report? Are they expected to report each and every event or only just specific types of events? To whom do they report? How are these events evaluated to decide if they qualify as incidents? Is there a classification scale? Is there a triage and/or escalation process to prioritize serious incidents? What is it based on?

A.16.1.5 Response to information security incidents: check what actions are taken once an incident is identified and prioritised. How is evidence collected, stored and evaluated? Is there an escalation matrix to use as needed? Are there means to communicate information of such incidents to internal and external organisations on a need-to-know/inform basis? Check actions taken to resolve and finally close the incident and record its occurrence.

A.16.1.6 Learning from information security incidents: check the evaluation/investigation mechanism in place to identify recurring or high impact incidents. How is the information gained from the evaluation of information security incidents used gainfully to prevent recurrence and implementing improvement opportunities? Also, is this used for awareness and training purposes? Check later parts of the processes for managing security incidents through to closure. Does the organization have a relatively mature incident management process in place? Is it proactively learning from incidents, improving risk knowledge and security controls accordingly? Check the records relating to recent incidents for evidence.

A.16.1.7 Collection of evidence: forensic collection of digital evidence is a specialised skill. Check whether this is done competently in-house or by third parties specialising and trained in this area. If retained in-house, confirm that there are trained, competent, trustworthy personnel with suitable tools and defined processes for the role (*e.g.* chain-of-evidence rigorously maintained, evidence secured in storage; analysis on forensically-sound copies using forensic-grade tools and techniques). Who decides to undertake forensics, and on what authority and basis? How are issues relating to jurisdiction, differing forensic standards and associated legal requirements (*e.g*. seizure, storage, analysis and presentation of evidence) handled?

A.17. Business continuity management (per ISO 22301)

A.17.1 Business continuity

This section reflects business continuity in general, not just the continuity of information security operations and controls in ISO/IEC 27002 section 17. Please refer to ISO 22301 and other guidance.

A.17.1.1 Business continuity planning: how does the organization determine its business continuity requirements? Review the associated policies, procedures, standards, guidelines, practices and records (*e.g.* business continuity plans). Determine whether suitable 'high availability' designs are employed for IT systems, networks *etc.* supporting critical business processes. Verify whether those involved understand the risks the organization is facing, correctly identify business critical processes and the associated assets, identify potential incident impacts, and mandate suitable preventative, detective and corrective controls. Evaluate business continuity plans, continuity exercises/tests *etc.* by sampling and reviewing the process documentation, reports *etc.* Verify that events likely to interrupt business processes will be promptly identified and assessed, triggering disaster recovery-type activities.

A.17.1.2 Implementing information security continuity: verify that suitable plans are in place to maintain business operations or restore them within defined timeframes following interruption or failure. Do the plans take into account the identification and agreement of responsibilities, identification of acceptable loss, implementation of recovery and restoration procedures, documentation of procedures and regular testing/exercises? Verify that there is a single coherent framework for business continuity planning. Verify whether the framework ensures that all plans are consistent and identify priorities for testing and maintenance. Determine whether the business continuity plans and the planning process, taken as a whole, are adequate to satisfy the identified information security requirements. Verify if business continuity plans are regularly exercised/tested to ensure that they are remain up to date and effective. Verify whether members of the crisis/incident management and recovery teams and other relevant staff are aware of the plans and are clear on their personal roles and responsibilities. Check that security controls at disaster recovery sites and alternative locations adequately mitigate the corresponding information risks (*e.g*. are the controls substantially equivalent to those at primary operational sites?).

A.17.1.3 Verify, review and evaluate information security continuity: check that business continuity policies and procedures include testing methods and frequency and evidence of actual testing and their results. Check whether the validity and effectiveness of information security continuity measures have been reviewed during the BC & DR execution, have any shortcomings been identified, have they (and how) been remediated and retested till the results are satisfactory?

A.17.2 Redundancies

A.17.2.1 Availability of information processing facilities: check how the availability requirements for ICT services are identified and satisfied. Verify resilience, capacity and performance arrangements, including monitoring and adjustments (*e.g*. dynamic load balancing). Examine incident records for clues about unreliable services, equipment, facilities, servers, apps, links, functions, organizations *etc*. Check that key information security controls are implemented and functional at disaster recovery/fall-back sites. If controls at DR/fall-back sites are less strict than those at primary sites, are the additional risks being treated appropriately (*e.g*. compensating controls such as increased oversight, and risk acceptance for the limited period of DR invocation)?

A.18. Compliance

A.18.1 Compliance with legal and contractual requirements

A.18.1.1 Identification of applicable legislation and contractual requirements: is there a policy on the subject (probably not specific to information risk, security and related areas but covering compliance in general)? Is there some form of compliance register or database maintained, listing *all* applicable legal, regulatory and contractual requirements obligations and expectations, each with accountable owners? Who owns, maintains, uses and controls the register? Are compliance requirements systematically identified and registered, both initially and any subsequent changes? *How* is compliance achieved and assured *i.e.* what activities are performed to meet the requirements and ensure they are met? For a sample of information security-related compliance requirements (*e.g.* privacy acts, intellectual property, PCI DSS, SOX, HIPAA, official secrets and relevant clauses in contracts, agreements and standards), ascertain whether the corresponding information security controls are in place. Check for example that suitable controls are in place to comply with requirements on:

- Privacy – soon including GDPR;
- Health and safety (most workers are valuable information assets!);
- The use of copyrighted materials such as licensed software (see A.18.1.2);
- Protection of important financial, tax and other business records against loss, destruction and falsification (*e.g.* fraud);
- Cryptography *e.g.* export controls.

A.18.1.2 Intellectual property rights: confirm that policies and procedures are in place concerning compliance with the associated requirements/obligations both by the organization and by second parties (*e.g.* licensees of corporate patents and copyright content). Check the permitted methods of acquisition and use of copyrighted materials, such as software licenses. Are there policies and procedures concerning acquiring, using and licensing intellectual property, license management, compliance reviews *etc*.?

A.18.1.3 Protection of records: check for a policy on records management that covers control requirements such as classification, categorisation, record types, retention periods, allowable storage media on which they are stored *etc*. Check also for the related cryptographic keys and digital signatures of such records which must also be securely stored. Ascertain how important organizational records are protected from loss, destruction and falsification, unauthorised access and release in accordance with statutory, regulatory, contractual and business requirements. Check whether the storage / archival arrangements take account of the possibility of media deterioration (*e.g.* controlled storage conditions, periodic integrity checks and/or transfer to fresh media)? Check if appropriate long-life storage media is used for long term storage.

A.18.1.4 Privacy and protection of personally identifiable information: check policies and procedures in this area. Check if these have been appropriately disseminated to all staff handling PII. Confirm who is the privacy officer of the enterprise and whether he/she is aware of what attributes of PII are collected and processed/stored by the organisation for organic employees, contractors and other third party staff? Confirm if the PII being collected is in line with legal and regulatory requirements, if the information assets on which PII is stored, processed and the channels for their communication have been identified, what are the access controls around such PII, what is the level of access and roles (of personnel) who have access on these assets *etc*.

A.18.1.5 Regulation of cryptographic controls: verify that the organization's use of cryptography is in compliance with all relevant laws, agreements/contracts and regulations. Check for a policy on the subject and if the organisation is involved in any import/export related activities of cryptographic material and/or encrypted information, and whether such activities are in compliance with legal and regulatory requirements. Check that the policy requires the organisation to comply with national legal mandates with reference to disclosure of encryption keys.

A.18.2 Information security reviews

A.18.2.1 Independent review of information security: are the organisation's information risk and security arrangements reviewed for suitability in line with its objectives by independent internal or external auditors? Are audit requirements involving checks on operational systems carefully planned, authorized, conducted and controlled to minimise risks to the business? Are audit objectives and scopes agreed and authorized by appropriate management? Is access to information system audit tools/software adequately controlled to prevent misuse and compromise? Are system audit tools prohibited from or protected on corporate systems, outside of authorized audits? Are audit findings recorded and acted on, and are audit records securely preserved for future reference?

A.18.2.2 Compliance with security policies and standards: how do managers and supervisors ensure that all security procedures within their area of responsibility are carried out correctly in compliance with security policies, standards *etc*.? Are there regular security compliance reviews within their area of responsibility?

A.18.2.3 Technical compliance review: are IT systems and networks regularly reviewed/tested for compliance with defined technical security requirements *e.g.* through network vulnerability scans and penetration tests? Check the corresponding policies, procedures, methods, tools and records. Are the tests conducted by appropriately qualified, competent and trustworthy professionals? Review the information risks and controls relating to the testing itself (*e.g.* legally binding obligations in contracts if external organizations are used; competent supervision, proactive/intense monitoring and thorough logging of activities). How are the results reported, analysed and used? Given their sensitivity, how are results secured? Review records of findings, analysis, prioritization, risk treatment decisions, change requests *etc*. to confirm that appropriate actions are in fact being taken to address identified issues. Cross-reference this with nonconformity and corrective action in B.10.1. Look out for longstanding, repeatedly reported issues that are evidently not being resolved.

Automated system security audit tools are powerful utilities but are not appropriate in all environments. They can potentially undermine system security, perhaps introducing additional technical vulnerabilities, extracting highly sensitive information and affecting system performance or availability. Furthermore, auditors using such tools must be competent to use and obtain meaningful data from them: a "pass" from an automated vulnerability assessment tool does *not* necessarily mean that a system is free of vulnerabilities and is hence secure. A wrongly-configured or ineptly used database security review tool may bring down a production system. Such tools should only be introduced using the organization's conventional change management processes, including pre-implementation risk assessment and security testing, where appropriate.

Appendix B - Generic ISMS *management system* audit checklist

Introduction

The following ISMS *management system* audit checklist comprises a generic set of audit tests. It is structured in line with and reflects ISO/IEC 27001's requirements for *all* ISMSs without regard to any *specific* requirements that an individual organization might have (for example legal, regulatory and contractual obligations concerning particular information risk and security processes, activities or controls).

Whereas ISMS certification audits are narrowly focused on the explicit wording of the standard, **this checklist is primarily intended to guide, or to be adapted and used by, competent internal auditors conducting ISMS internal audits**. It can also be used for internal management reviews of the ISMS including pre-certification assessments to determine whether the ISMS is in a fit state to be formally audited. That said, internal audits and management reviews along these lines should help the organization prepare and finalize the necessary documentation that certification auditors will probably want to review.

This audit checklist is NOT intended for certification audits. Certification auditors are required to follow their formally-documented and accredited audit processes, using their own audit checklists and audit tests concerning the extent to which the ISMS complies with the requirements specified in ISO/IEC 27001.

Internal audit checklists may be further modified during the course of the audit if new or previously unappreciated areas of concern come to light. Unlike strict compliance audits, internal audits *may* delve into related issues that emerge as the audit proceeds, within the more flexible boundaries of the scope, timescales and resourcing available.

The extensive audit tests suggested below in the form of questions and checks are intended as prompts or reminders of the main aspects to be checked by competent, qualified and experienced IT auditors. They do not cover every single aspect of ISO/IEC 27001. They are not meant to be asked verbatim and simply checked-off, whether in whole or piecemeal. They are not suitable for use by inexperienced auditors working without supervision.

This checklist is **not** meant to be used without due consideration and modification. It is anticipated that users will normally generate custom checklists reflecting the specific scope and scale of the particular ISMS being audited, and the audit tests arising, taking into account any information security requirements that are already evident at this stage (such as information-security relevant laws, regulations and standards that are known to apply to similar organizations in the industry).

Finally, checklists should support the auditors' normal working practices, for example in a tabular format with additional columns for the auditor to record notes and commentary, initial evaluation (*e.g.* SWOT/PEST/PESTEL), references to audit evidence on file, maturity metrics *etc*. Once completed, the audit checklist links the audit evidence and findings gathered and analysed during the fieldwork and analysis phases through to the audit report.

Since completed ISMS audit checklists, files, notes and evidence contain sensitive information concerning the organization's information risk and security arrangements, they *must* be adequately secured to ensure their confidentiality and integrity.

B.4. Context of the organization

B.4.1 Understanding the organization and its context

Has the organization identified a number of external and internal issues that are relevant both to the purposes of the organization and to the ISMS? How well are these described in the ISMS scope? How relevant and important are they? Is there a strong impression that information is a business asset, information risk is a business issue, information security supports the business in achieving its objectives, and hence the ISMS is a valuable business-enabling governance structure?

B.4.2 Understanding the needs and expectations of interested parties

If the ISMS scope only covers *part* of the organization, the remainder is probably an 'interested party' with needs and expectations relevant to the ISMS.

Carefully consider the ISMS scope and related documents. Has the organization identified external stakeholders or parties outside the scope of the ISMS with an interest in the organization's information risks and security arrangements? Check that all relevant interested parties have been identified and duly considered *e.g.* suppliers; business partners; customers and prospects; workers; governments, authorities and regulators; owners; professional advisors; reviewers and auditors; decision makers; local communities and society at large. Check that *their* information risk and security requirements been determined and taken into account in the ISMS, in addition to the organization's own *e.g.*:

- ISO/IEC 27001 certification of the organization's ISMS by an accredited certification body;
- Applicable laws and regulations *e.g.* privacy, finance and tax laws; official secrets and freedom of information acts;
- Contractual obligations, liabilities and constraints *e.g.* licenses for intellectual property;
- Security (particularly confidentiality but also integrity and availability) of confidential personal and proprietary information;
- Reliability, performance and capacity of information and information services *e.g.* Internet and cloud service providers; information feeds;
- Identifying, responding to and reporting information security incidents or breaches;
- Enabling and limiting the information risks associated with various business activities and IT operations, supporting business objectives such as governance, profitability and continuity;
- Maintaining a fit-for-purpose operational infrastructure and services (*e.g.* systems maintenance and software support);
- Gaining assurance that the organization is competently, efficiently and effectively identifying and treating information risks.

There is common ground between internal and external drivers for information risk and security, since information is a vital business asset. This section emphasizes the external perspective.

B.4.4 Information Security Management System

Check this detailed list of mandatory and recommended documentation from the free ISO27k Toolkit.

Compile and check the documentation and other evidence concerning the establishment, implementation, maintenance and continual improvement of the ISMS including mandatory ISMS documents and records arising from the management processes, metrics and trends demonstrating improvement, results of management reviews and decisions taken at such reviews *etc.* Has management authorized the implementation and operation of the ISMS, for example through a formal memorandum, project approval, letter of support from the CEO *etc.*? Was this a mere formality or is there evidence that management genuinely understands and supports the ISMS?

B.5. Leadership

B.5.1 Leadership and commitment

Evaluate the extent to which the organization's management leads and supports the ISMS based on evidence such as:

- Discussions, interviews, meetings *etc*. with management on and around this topic;
- Memoranda, emails, presentations, briefings *etc.* through which management expresses support for and commitment to the ISMS and acceptance of ISMS objectives and implementation plans;
- The allocation of adequate resources and prioritization of the activities associated with designing and building, implementing, operating and maintaining the ISMS (going beyond vocal support, is the organization proactively investing in it?);
- Clear management direction where appropriate, such as risk acceptance criteria, risk appetite/tolerance relating to information risk;
- Management-level interest and participation in ISMS activities such as meetings, workshops, focus groups, policy development and approval, awareness activities and training courses, reviews and audits;
- Management's prompt and positive responses to challenges, issues and concerns, incidents, recommendations, tests and exercises, management review and audit reports *etc*.;
- Indications that workers in general understand the importance of the ISMS and willingly accept their roles within it (implying a corporate security culture).

B.5.2 Policy

Review the information security policy suite and related documentation (*e.g.* ISMS mission statement and scope). Check that it:

This section concerns the *governance* aspects: corporate policies must be driven and mandated by management. The *content* of the information risk and security policies is specified in ISO/IEC 27002 section 5.1.1.

- Explicitly supports and enables the business purposes and objectives of the organization, in the context of information risk, security and related requirements (*e.g.* compliance, protection, safety and business continuity);
- Specifies high-level information risk and security objectives, both internally and externally driven or imposed, and clearly affirms the organization's commitment to satisfy them;
- Is sufficiently formal and explicit to stand up in legal or disciplinary proceedings, yet readable and pragmatic enough to be useful in practice (albeit supported by procedures, guidelines *etc*.);
- Supports continual improvement of the ISMS, reflecting the evolving information risks and business situation, and maturity;
- Is approved, authorized and/or mandated as a coherent and reasonably comprehensive suite by "top" (senior) management *e.g.* board, CEO, Executive Committee or Security Committee;

Individual policies, procedures *etc*. may be owned and authorized at lower levels, but the overall structure needs senior management's explicit leadership and mandate *e.g.* through an overarching corporate strategy or policy on information risk and security.

- Is communicated widely within the organization, including everyone within the scope of and directly implicated in the ISMS;
- Is, where appropriate (possibly under nondisclosure agreements or in summary form) made available to other interested parties.

B.5.3 Organizational roles, responsibilities and authorities

Check whether information risk and security-specific roles are assigned, and related accountabilities, responsibilities and authorities are defined and communicated *e.g.* in job descriptions and roles and responsibilities documents specifying key activities, necessary competences and qualifications *etc*. Are key responsibilities and authorities (*e.g.* compliance, metrics, authorizations, reviews and audits) appropriately assigned? Are there suitable, competent people in key roles?

Accountability is a valuable control approach. Holding people personally accountable for their decisions, actions and inactions reinforces their obligations, for example to protect information in their care.

Review the information risk and security management structure. Compared to other business activities and functions, is information risk and security given sufficient emphasis and management support? Is there evidence of a powerful ‘driving force’ at senior management level such as a management committee or forum to discuss information risk and security policies, risks and issues, and take key decisions? Is there sufficient budget for information risk and security activities? Are information risk and security-related activities effectively co-ordinated and aligned among the various business units, departments, functions, teams, individuals and external parties with interests in this area? Are the information flows (*e.g.* incident reporting and escalation) operating effectively in practice?

B.6. Planning

B.6.1 Actions to address risks and opportunities

B.6.1.1 General

Check whether internal and external issues, as well as interested parties' requirements, are considered while planning for ISMS and related risks and opportunities are considered (see also 4.1 and 4.2). Is there a documented [information] risk management process to identify, assess/evaluate (according to estimated probabilities and impacts) and treat information risks? Are the criteria for deciding on risk treatment options clear, including the pros and cons of different approaches and risk appetite/tolerance levels?

B.6.1.2 Information security risk assessment

Ascertain and review the organization's choice/s of information risk assessment method/s, whether bespoke or generally-accepted methods. Are the results of risk assessments comparable and reproducible? Look for examples of anomalous or counterintuitive results to determine how they were addressed and resolved. Was the risk assessment method updated as a result? Check that ‘risk scenarios’ are described for each risk, ‘risk levels’ are assigned based on qualitative or quantitative measurement, ‘risk owners’ are nominated, and risks are prioritised for treatment? Have recent changes (*e.g.* new/updated IT systems, business processes and relationships) been suitably risk assessed? Are the **R**isk **T**reatment **P**lan, **S**tatement **of** **A**pplicability, policies and procedures *etc*. being used proactively as information risk management tools?

B.6.1.3 Information security risk treatment

Review the organization's RTP. Are appropriate treatments specified for all identified information risks *i.e*. **avoiding** risks by not undertaking risky activities; **reducing** risks through suitable controls; **sharing** risks with third parties such as insurers; or **accepting** risks that fall within management's risk appetite? Check that risk owners have approved the RTP and accepted the residual risks. Look for gaps, overlaps and other anomalies (*e.g*. seemingly inappropriate or ineffective treatments). Check how the RTP relates to the **S**tatement **o**f **A**pplicability specifying the following for controls recommended in ISO/IEC 27001 Annex A and/or other standards, control catalogues *etc*.:

- Whether it is applicable (include the justification if not);
- Whether it arises from a legal, regulatory or contractual obligation, or is business-driven (*e.g*. addresses an information risk of concern to the business, or good practice);
- How it addresses the risk (*e.g*. preventive, detective or corrective; technical, procedural, physical or legal *etc*.).

ISO/IEC 27002 *may* be restructured to identify categories or types of security control. Doing so now puts the organization ahead of the game!

B.6.2 Information security objectives and planning to achieve them

Review the ISMS mission, objectives, goals, strategies, plans *etc*. Does the ISMS explicitly support the organization's strategic business objectives? Do the ISMS objectives reflect the organization’s key information assets and risks, plus its legal, regulatory, contractual and other external obligations in this area?

Consider for each objective:

- What, exactly, is the objective? What are we aiming to achieve or avoid here? What is driving this – its purpose and value?
- How will we know whether it has been achieved? How will progress and results be measured and evaluated (metrics plus success/failure criteria)?
- What will be done to achieve it? What resources are required?
- Who is accountable for achieving it, by what means, and by when?

Look for objectives to be **S**pecific, **M**easurable, **A**chievable, **R**elevant and **T**imebound.

B.7. Support

B.7.1 Resources

Review the resources allocated to the ISMS in terms of budget, manpower *etc.*, in relation to the organization's stated aims for the ISMS and (where applicable) by comparison to comparable organizations (benchmarking). Is the ISMS adequately funded and resourced in practice? Are sufficient funds allocated by management to address information security issues in a reasonable timescale and to a suitable level of quality?

B.7.2 Competence

Review the qualifications, experience and training of those specifically involved in operating the ISMS, and general information security awareness activities targeting all employees. Are necessary competencies and training/awareness requirements for information security professionals and others with specific roles and responsibilities explicitly identified and provided? Are training/awareness budgets adequate to fund the associated training and awareness activities? Review training evaluation reports *etc*. and seek evidence to confirm that any necessary improvement actions have in fact been taken. Check by sampling that employee HR records note ISMS-related training *etc*. (where applicable). Assess the general level of information security awareness by surveying/sampling, or review the results of surveys/samples conducted as part of the ISMS.

B.7.3 Awareness

Are information security policies *etc*. well written and disseminated appropriately to all relevant parties? Are recipients explicitly required to read and comply with them? How does the organisation confirm that all have in fact read and agreed to comply with the policies *e.g*. signed acceptance or acknowledgement; periodic quizzes/tests to confirm that recipients understand their obligations, including their wider role in information risk management and making the ISMS effective and beneficial for the organisation? How are policy compliance and non-compliance addressed *e.g.* benefits/rewards to reinforce compliance and costs/penalties for non-compliance, through disciplinary procedures, relationship/contractual management *etc*.? How are changes communicated *e.g.* new or revised policies, roles and responsibilities, information risks (*e.g.* novel threats) and security controls? Is management sufficiently engaged and supportive *e.g*. do managers actively participate in information risk and security awareness activities, training courses *etc*.? Are training and awareness plans, budgets and priorities adequate?

B.7.4 Communication

Is there a documented communication plan identifying internal and external audiences to whom appropriate and timely communication must be made with respect to all activities and occurrences related to information security *e.g.* employees (need clear directions of what is expected of them, updates on policies, training in procedures *etc*.); third parties/suppliers (need clear directions about what is expected of them; and legal and regulatory authorities plus certification body and other stakeholders (need to be notified in the event of breaches or incidents). Does the communication plan state what is to be communicated, when (timing or frequency), by whom and by what means? Is there evidence confirming that previously planned communications have taken place and been effective?

B.7.5 Documented information

B.7.5.1 General

Check for all the 'documented information' (= documentation!) explicitly required by ISO/IEC 27001 (*e.g.* ISMS scope, roles and responsibilities, risk assessment, Statement of Applicability, Risk Treatment Plan, risk register, evidence of management reviews, internal and external audit reports) and associated documentation (NCRs *etc*.). Has management identified any additional documentation necessary for effectiveness of the ISMS and is it available? How is ISMS information made available where needed (*e.g*. an intranet-based policy management system, SharePoint repository and/or on paper)?

Reminder: mandatory and recommended documentation

B.7.5.2 Creating and updating

Is the process for creating, updating and authorizing or mandating compliance with documentation suitably controlled? Check for the presence of, and compliance with, policies and procedures for controlled and authorized updates to ISMS documentation, policies, procedures, records *etc*. (How) are ISMS documentation changes managed and controlled *e.g*. changes reviewed and approved by relevant managers, and promulgated appropriately? Is document metadata standardised and adequate *e.g.* document title, name of owner, date of publication, date of last and next review, distribution *etc*.? Is there a list, inventory or database of controlled documentation?

B.7.5.3 Control of documented information

Further to 7.5.2, is important ISMS-related documentation adequately secured and protected (*e.g.* access control, version control, a defined retention and revision policy, backups *etc.*)? Evaluate the controls protecting important ISMS records such as various information security review and audit reports, action plans, formal ISMS documents (including changes to same), visitors' books, access authorization/change forms *etc*. Review the adequacy of controls over the identification, storage, protection, retrieval, retention time and disposition of such records, particularly in situations where there are legal, regulatory or contractual obligations to implement an ISO27k ISMS (*e.g*. to protect personal data or to supply a certified organization).

Are important documents of external origin clearly identified as such and suitably controlled?

B.8. Operation

B.8.1 Operational planning and control

Check the plans in place to monitor and control all ISMS activities including continuous risk management (see B.6.1) and actions to achieve information security objectives (see B.6.2). The information risk management activities should cover commercial information services such as cloud computing where applicable.

B.8.2 Information security risk assessment

Check that the ISMS-wide information risk assessment is repeated or at least reviewed and updated at suitable intervals (*e.g*. annually or in the event of any significant change) to address any changes in threats, vulnerabilities or impacts and hence risk levels. Review actions taken in response to previously-identified changes in the risk levels. Are risk assessments and reviews documented appropriately *e.g.* records of risks identified and treatments selected; who reviewed what and when; output reports and action plans, ideally identifying those responsible and priorities/timelines?

B.8.3 Information security risk treatment

Review the **R**isk **T**reatment **P**lan. It should record management decisions to treat every identified information risk through one or more defined forms of risk treatment:

1. **Avoid:** management typically decides not to do some activities at all (or at least not now) if the information risks are considered too high relative to the business advantages of proceeding. What prevents someone going ahead with these activities anyway, regardless of the formal decision to avoid the risks?;
2. **Reduce:** information risks that are to be reduced (mitigated or ameliorated) should be listed in the RTP along with details of how the risks will be reduced, typically through information security controls. Other details typically recorded in the RTP include who is responsible for reducing the risk, the dates by which controls are to be fully implemented and risks are to be reduced, who will or has reviewed/checked and confirmed that risks have been sufficiently reduced *etc.*;
3. **Share:** if information risks are to be shared with (partially or wholly transferred to) third parties, check that the documentation includes terms in contracts, agreements or cyberinsurance policies clarifying obligations and liabilities relevant to information risks; security, privacy, compliance, incident notification and management aspects including business continuity; right of audit; metrics *etc.*

4. **Accept:** all information risks that remain after the above treatments (including any that were not identified, or where the risk treatments fail or fall short in some way) *have* to be accepted by the organization. In addition, management may explicitly choose to accept some information risks. Check how the residual and accepted risks are identified and managed *e.g.* assigned to appropriate accountable risk owners, monitored and reviewed at predetermined intervals. Look for linkages to incident management, business continuity, disaster recovery and all-purpose contingency arrangements.

B.9. Performance evaluation

B.9.1 Monitoring, measurement, analysis and evaluation

(How) does management monitor the ISMS to ensure that the security controls identified in the RTP, SoA, policies *etc.* are effectively implemented, in operation and achieving objectives? How does management promote and support continual improvement of information risk and security management, driving the maturity of the ISMS while remaining aligned with business objectives?

Review the ISMS monitoring and measurement activities using evidence gleaned from: security metrics; minutes of meetings and actions arising; management review and internal audit reports; breach/incident reports; security investment or project proposals, business cases *etc.*

Check how the metrics are specified/defined and used *e.g.* data sources; data collection, analysis and reporting frequencies; who collects, analyses and present/reports the data, and to whom. Consider the purpose, quality, utility and value of the metrics *e.g*. using the PRAGMATIC criteria. Taken as a whole, do the metrics present a reasonably comprehensive, accurate and timely perspective to management? Are key management decisions driven by the metrics, in fact?

[How] do the metrics drive continuous improvements?

Metrics support decisions by addressing questions relating to or arising from goals and objectives. High-level metrics concerning the ISMS itself typically measure its effectiveness and value to the organization, its compliance with and achievement of various requirements, mid- to long-term trends, resourcing and priorities, its implementation status and maturity *etc.* in the organization's broader business context. Low-level detailed metrics used within the ISMS to manage information risks, security controls, incidents *etc*. depend heavily on the particular situation, and tend to be more operational/short-term in nature. See ISO/IEC 27004:2016 for more.

B.9.2 Internal audit

Review the organization's internal audits of the ISMS as documented in ISMS internal audit scopes, plans, reports, action plans *etc*. Is there an ISMS internal audit programme, showing a planned set or series of audits? Are responsibilities for conducting ISMS internal audits formally assigned to competent, adequately trained auditors (contractors or consultants if no suitable employees are available)?

To what extent to internal audits confirm that the ISMS meets its requirements defined in ISO/IEC 27001 plus relevant legal, regulatory or contractual obligations, and organizational ISMS requirements specified through the risk assessment process?

Check that recommendations, action plans, corrective actions *etc*. are generally being addressed and verified within agreed timescales, paying particular attention to any currently overdue actions for topical examples.

It is not uncommon for some agreed actions to remain incomplete at the planned completion dates, especially if they are complex, costly or involve other parties. The point is not that everything must be done exactly as planned so much as that management remains on top of the situation, proactively managing the work and allocating sufficient resources to achieve a sensible rate of progress, with a reasonable proportion of agreed actions being completed on time. Continuous improvement and positive business outcomes are more important than strict adherence to plans – see also section 8.

B.9.3 Management review

Management reviews of the ISMS should occur at least biannually or whenever there is a significant change to the ISMS. Is this defined *e.g*. in policy? When has management previously reviewed the ISMS, and when does it next plan to do so?

By reviewing management reports and other records, and/or by interviewing those who were involved, check what went in to the previous management review/s (ISO/IEC 27001 identifies nine items such as the results of other audits/reviews, feedback and improvement suggestions, information on vulnerabilities and threats *etc*.). Assess the extent to which management played an active part and was fully engaged in the review/s.

Whether an ISMS certification audit, performed at management's request, could be considered a "management review" strictly within the terms of the ISO/IEC standard is unclear, but that was not the intent. Their objectives and processes differ *e.g*. audits are formalized, independent assessments, whereas management reviews may not be.

Check the outputs of any previous management review/s including key management decisions, action plans and records relating to the confirmation that agreed actions were duly actioned. If necessary, confirm that closed actions have in fact been properly completed, focusing perhaps on any that were not completed on time.

B.10. Improvement

B.10.1 Nonconformity and corrective action

Review a sample of records to evaluate what actually happens when a nonconformity is detected *e.g*. through a review, audit, near-miss or incident. Are they routinely and consistently documented in the form of **N**on-**C**onformance **R**eports (**NCR**s) including:

- Explicit details of the non-conformance including which obligations, requirements or controls it relates to (*e.g*. clauses of ISO/IEC 27001; policies; laws and regulations; contractual terms; insurance conditions; good practices);
- Root cause analysis, digging into the underlying reasons, gaps, issues or failures that allowed the situation to occur;
- Actions planned to address root causes, including any changes to ISMS strategies, policies, procedures, priorities, resourcing, controls, metrics, oversight *etc*.;
- Specification, prioritization, scheduling/planning and resourcing of the actions arising;
- Evidence demonstrating that the NCR has in fact been addressed and resolved;
- Independent confirmation that the NCR has been resolved and hence can be closed?

Aside from the obvious but often superficial symptoms and reactive aspects (such as compliance for the sake of it), it is worthwhile diagnosing and proactively treating any underlying root causes in order to prevent issues from recurring and perhaps worsening, like a cancer.

Are appropriate corrective actions fully implemented and their effectiveness reviewed, routinely? Does anyone make the effort to determining whether similar nonconformities exist, or may occur, elsewhere? Are nonconformities and corrective actions considered in management reviews (B.9.3)?

B.10.2 Continual improvement

In addition to making ISMS improvements in response to reported nonconformities, does the organization takes a more proactive stance towards addressing potential improvements, emerging or projected new requirements *etc.*? How are potential ISMS improvements identified, assessed and (if applicable) implemented? Obtain and review records relating to corrective actions such as reports and action plans from ISMS management review/s or audits (see 9.2 and 9.3), ISMS change requests, budget/investment proposals and business cases *etc*. Seek evidence that the ISMS is, in fact, being materially improved in response to emerging or projected new requirements, emerging good security practices *etc*. Seek evidence of ISMS changes (such as adding, changing or removing information security controls) corresponding to significantly changed information risks.